UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

YGOR VOLTOLINI DA SILVA

REFORÇANDO A SEGURANÇA EM AMBIENTES VOIP QUE UTILIZAM CENTRAIS TELEFÔNICAS PRIVADAS

MONOGRAFIA

CURITIBA
2012

YGOR VOLTOLINI DA SILVA

REFORÇANDO A SEGURANÇA EM AMBIENTES VOIP QUE UTILIZAM CENTRAIS TELEFÔNICAS PRIVADAS

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Augusto Foronda

CURITIBA

2012

Aos meus pais, José Roberto da Silva e Roseli Aparecida Voltolini, que sempre foram, são e serão exemplos de dedicação, educação e amor.

À minha namorada, Fernanda Portela, e a todos os meus amigos, que são o meu porto seguro, fontes inesgotáveis de inspiração.

RESUMO

SILVA, Ygor Voltolini da. **Reforçando a segurança em ambientes VoIP que utilizam centrais telefônicas privadas.** 2012. 57 f. Monografia (Especialização em Gerenciamento de Redes) – Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Esta monografia tem o intuito mostrar como os principais e mais conhecidos mecanismos de segurança atuam nas comunicações VoIP. Para tal, é utilizada a base de centrais da linha HiPath 3000 da Siemens Enterprise, sobre as quais são recriados ambientes de comunicações entre ramais IP, com operadoras VoIP autenticadas via protocolo SIP e, por fim, interligadas à outras centrais telefônicas. A premissa deste estudo é instruir projetistas, engenheiros e técnicos na área de telecomunicações de como pode enrijecer a segurança em comunicações de voz na internet, de forma a evitar roubos de senhas de acesso, ataques de intrusos e, por consequência, a quebra de sigilo nas comunicações privadas.

Palavras-chave: VoIP. Segurança. SIP. Centrais Telefônicas.

ABSTRACT

SILVA, Ygor Voltolini da. **Reinforcing security on VoIP environments which uses PBX.** 2012. 57 p. Essay (Graduate Certificate in Networking and Systems Administration) - Federal Technological University of Paraná. Curitiba, 2012.

This essay has the goal show how the main and most known security mechanisms act on VoIP communications. For this, the HiPath 3000 PBX line, of Siemens Enterprise, is used, to reproduce communications environments between IP subscriber lines, with ITSP authenticated using SIP protocol and, lastly, interconnected to other PBX. This study premise is instruct projectists, engineers and technicians who works in telecommunications about how to improve voice communications over internet security, avoiding password robberies, intrusion attacks and, as result, invasion on private communications.

Keywords: VoIP. Security. SIP. PBX.

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA

A preocupação com a segurança nas redes IP vem crescendo exponencialmente. Medidas legais, como penas severas para criminosos virtuais, já são uma realidade. Os gerentes de redes mais do que nunca estão implantando soluções como detecção de intrusos, firewalls com filtros avançados, anti-vírus, chaves de criptografia, proxy, entre outros.

Na telefonia baseada na internet, também chamada de VoIP (*Voice over IP*), não é diferente. Os invasores deste tipo de sistema, também chamados de *phreakers*, estão atuando silenciosa e perigosamente, ameaçando não só com a interceptação das ligações, como também derrubando as comunicações de voz via centrais telefônicas das corporações, através dos ataques de negação de serviço.

O intuito deste estudo é mostrar como se prevenir dos ataques mais comuns, utilizando mecanismos de segurança disponíveis na linha de PBX Siemens HiPath 3000. A segurança não será aplicada de forma a garantir total confiabilidade em relação a possíveis ataques, pois este é um cenário utópico; porém, será mostrada a prevenção ideal com as ferramentas existentes num equipamento consolidado no mercado.

1.2 DELIMITAÇÃO DA PESQUISA

São apresentados, na teoria, os tipos de ataques comuns em redes IP e os mecanismos de prevenção aos ataques mencionados. No capítulo seguinte, quais são as maiores ameaças em VoIP e a solução para a enrijecer a segurança contra tais.

Dando sequência, serão apresentados os mecanismos existentes no sistema de mercado utilizado de referência e suas respectivas configurações para três cenários: ligações relacionadas de ramais IP; chamadas recebidas ou efetuadas através de uma operadora VoIP; estabelecimento de chamada e tráfego de voz em duas ou mais centrais interligadas utilizando a rede IP.

O grande destaque do estudo é a possibilidade de configuração e uso de vários meios de segurança simultaneamente, isto graças ao conhecimento teórico passado no segundo capítulo deste.

Da parte dos *phreakers*, após o enrijecimento da segurança implementado neste projeto, caberá ter um elevado conhecimento de como quebrar estes mecanismos, e ainda será imprescindível um esforço computacional muito grande, além de tempo para processamento para descriptografar as longas chaves de acesso. Ou seja, do ponto de vista prático, será muito difícil de serem rompidas tais barreiras.

1.3 PROBLEMA

As redes de voz sobre IP começaram a ser implantadas em corporações no final da década de 1990. Naquele tempo, mal existia estrutura para a implantação de redes deste tipo. Pensar em segurança não era comum, uma vez que os primeiros ataques de redes IP conhecidos num âmbito mundial ocorreram a partir dos anos 2000, como por exemplo o vírus "*I love you*". Apesar de, a partir desta época os cuidados com segurança terem crescido a cada ano, não se importava muito com a segurança nas redes IP de voz.

Porém, a partir da segunda metade dos anos 2000, ataques às redes VoIP foram sendo divulgados e se tornaram cada vez mais frequentes. Assim, os dispositivos de voz sobre IP, se não tinham ferramentas de segurança, passaram a ter; os que já tinham, aprimoraram.

Este estudo é trazido à tona para sanar muitas dúvidas sobre quais são as providências a serem tomadas, se elas realmente evitarão ataques e os ônus de tais implantações.

1.4 OBJETIVOS

A seguir, serão apresentados os objetivos geral e específicos, que se pretende atingir com este projeto de pesquisa.

1.4.1 Objetivo Geral

Realizar um estudo sobre a segurança num ambiente corporativo que utiliza o VoIP através de centrais telefônicas.

1.4.2 Objetivos Específicos

Os objetivos específicos são:

- Pesquisar os tipos de ataques existentes para redes VoIP;
- Pesquisar os mecanismos existentes para combater os ataques à redes VoIP;
- Mostrar a configuração de um PBX de mercado com segurança nas suas comunicações de voz sobre IP;

1.5 JUSTIFICATIVA

Baseado na crescente demanda dos gerentes de TI e diretores de empresa, em tornar toda e qualquer comunicação via rede IP confiável e segura, independente se for de dados ou voz, e também no fato de ataques estarem ocorrendo com frequência, este trabalho está pautado em sugerir grandes melhorias quanto à segurança na comunicação de voz sobre IP. Prova desta necessidade pode ser vista na matéria trazida no link http://g1.globo.com/tecnologia/noticia/2010/06/pacotao-de-seguranca-phreaking-recycler-e-filmes-sobre-hacking.html, na qual além de dizer sobre as ameaças típicas de uma rede de dados, também cita a preocupação com a rede de telefonia IP.

1.6 PROCEDIMENTOS METODOLÓGICOS

Como material de apoio, são referenciados livros nas áreas de segurança de redes IP em geral, específicos na área de segurança em redes VoIP, sobre interconexão de redes LAN pela rede WAN, além de normas e RFCs (*Requests For Comments*) sobre os mecanismos de segurança abordados.

Este trabalho também traz a implantação dos parâmetros recomendados de segurança numa central telefônica de mercado. Para tal, foi escolhida a linha de centrais HiPath 3000, da Siemens Enterprise.

Não é parte desde estudo a elaboração de uma cartilha sobre como configurar a segurança em qualquer tipo de PBX, pois esta dependerá do equipamento utilizado e da estrutura de redes disponível na corporação, além da análise de custos *versus* benefício da solução.

1.7 ESTRUTURA

Esta monografia é estruturada por 5 capítulos complementares entre si, que visam satisfazer os objetivos propostos. No capítulo 1, capítulo introdutório a seguinte estrutura é formulada tendo início com: i) tema; ii) delimitação da pesquisa; iii) problema; iv) objetivos; v) justificativa; vi) procedimentos metodológicos; vii) estrutura.

Para desenvolvimento do tema proposto foram sugeridos os capítulos 2, 3 e 4 que englobam as teorias e práticas desta pesquisa. No capítulo 2 traz um estudo geral sobre as ameaças de ataques mais comuns sofridas pelas redes IP em geral. O capítulo 3 traz um estudo específico sobre a segurança em redes VoIP, detalhando as ameaças possíveis e os mecanismos de segurança mais comuns para evitar tais invasões.

A parte de configuração de um sistema real de comunicação VoIP de mercado concentra-se no capítulo 4, na qual serão detalhados vários parâmetros de segurança para as centrais da linha de PBX Siemens HiPath 3000.

No capítulo 5 é apresentada a conclusão da monografia e suas considerações futuras, descrevendo os resultados, aplicabilidade e utilização da segurança em ambientes VoIP.

2 COMO ATACAR UMA REDE VOIP

Os ataques às redes convergentes, ou redes puramente VoIP, estão cada vez mais comuns. Os ataques da infraestrutura de rede - negação de serviço, escuta e interceptação telefônica, envenenamento de DNS (*Domain Name Server* – Servidor de Nome de Domínio) e cópia da tabela ARP (*Address Resolution Protocol* – Protocolo de Resolução de Endereços) são os mais frequentes.

Além dos ataques relacionados à infraestrutura de rede, este capítulo traz outros tipos de ataque, como os relacionados aos protocolos de conexão e tráfego.

2.1VIA PROTOCOLO DE CONEXÃO SIP

Muitos são os tipos de ataques envolvendo o protocolo de conexão SIP (*Session Initiation Protocol* – Protocolo de Início de Sessão), porém o foco de estudo é nos dispositivos que o utilizam para estabelecer ajustes na sessão. A seguir, lista dos quais são estudados:

- Sequestro de registro;
- Quebra de senha (ataque por dicionário);
- *Man-in-the-middle* (invasor no meio da negociação SIP);
- Enumeração do nome de usuário;
- Clone dos servidores Registrar e Proxy;
- Negação de Serviço (*Denial of Service, DoS);*

2.1.1 Sequestro de registro

Este tipo de ataque tira vantagem da habilidade que o Agente Usuário (*User Agent*) tem de modificar o campo de Contato (*Contact*) no cabeçalho SIP. Uma vez este campo modificado por uma entidade intrusa, ele pode se registrar como Agente Usuário no SIP registrar e, com isto, os servidores SIP Proxy poderão encaminhar as requisições de conexão INVITE para um telefone IP, ou para um *Gatekeeper*.

A modificação do campo de Contato no cabeçalho SIP é feita da seguinte forma: o invasor envia uma requisição de registro exatamente igual à capturada num pacote do usuário

válido, porém com o campo de *IP address* de origem modificado para o seu próprio IP. Desta forma, o campo de contato é reconhecido.

O melhor método de clonar uma mensagem de requisição SIP é com uma ferramenta chamada SiVuS. Esta é capaz de descobrir redes SIP, dispositivos autenticados, e criar mensagens SIP.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.1.2 Quebra de senha (Ataque por dicionário)

O protocolo SIP envia a sua senha de autenticação utilizando o algoritmo de desafio MD5. O invasor, por sua vez, pode capturar os pacotes na rede utilizando um programa de mercado comum, como por exemplo o *Wireshark*, para capturar dados como o usuário, o *realm*, o *method*, a URI, e a resposta para a autenticação com o *hash* MD5 (*Hash Message Digest 5* – Mensagem de resposta do algoritmo). Com posse destes dados, o invasor pode tentar um ataque de dicionário, ou seja, palavras prováveis para a senha inserida. Com estas palavras geralmente são curtas, como por exemplo, o número de um ramal de um PABX, o esforço necessário é mínimo. Estas tentativas podem ser feitas *offline*, uma vez que o intruso tem posse destes dados a partir da captura dos pacotes. Quando o ataque for feito, ele já terá os dados necessários para efetuar o ataque com sucesso já na primeira vez, eliminando as chances de medidas corretivas por parte do administrador da telefonia IP.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.1.3 *Man-in-the-middle* (invasor no meio da negociação SIP);

Para este ataque, o invasor pode utilizar duas técnicas: envenenamento da tabela ARP, ou clonagem do DNS. Com qualquer uma delas, consegue-se a permissão para estar entre o servidor SIP e o Agente Usuário. Com este tipo de ataque, o intruso não precisa necessariamente conhecer *usernames* e *passwords* válidos; basta rotear o tráfego entre servidor e cliente e agir interceptando os pacotes, impedindo-os de chegar ao seu destino real,

que é o servidor SIP. Para dar a impressão ao Agente Usuário de que sua requisição de autenticação foi aceita pelo servidor, o atacante envia mensagens de sucesso ao requerente.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

2.1.4 Enumeração do nome de usuário

Este método se utiliza de dados dos usuários para garantir um ataque com sucesso. Existem duas formas possíveis destes dados serem obtidos:

- Utilizando mensagens de erro;
- Utilizando a captura de pacotes;

No primeiro método, os dados dos nomes dos usuários podem ser identificados por mensagens de erro enviadas pelos servidores Proxy e *Registrars* (Registros) do protocolo. Com elas, o usuário pode enviar ataques por força bruta, tentando a autenticação com uma lista de nomes de usuários. Caso ele obtenha mensagem para uma tentativa, ele pula para a próxima tentativa da lista, até ter sucesso.

No método de captura de pacotes, o invasor pode capturar os pacotes da rede que são passados em texto claro. O mais útil deles é o que contém a URI SIP, que tem o formato *SIP:User@hostname:port*. Nota-se que, com esta simples ação, conseguiram-se o nome do usuário, o endereço IP do usuário e a porta de conexão utilizada.

Referência: ROSENBERG, J. et al. **RFC 3261:** SIP: Session Initiation Protocol. IETF, 2002.

2.1.5 Clone dos servidores Registrar e Proxy

Durante um registro, um Agente Usuário envia uma mensagem REGISTER para um servidor SIP Proxy ou SIP Registrar. Um invasor pode falsificar uma resposta a partir dos domínios destes servidores e redirecionar o Agente Usuário para um servidor SIP Proxy ou Registrar que ele mesmo controla, podendo assim receber chamadas telefônicas do Agente Usuário, gravá-las e utilizar tais ações da forma que lhe convir.

Referência: ROSENBERG, J. et al. **RFC 3261:** SIP: Session Initiation Protocol. IETF, 2002.

2.1.6 Negação de Serviço (*Denial of Service, DoS)*

Os três meios mais utilizados para um ataque de negação dos serviços são:

- Via mensagem de resposta BYE;
- Via mensagem de resposta REGISTER;
- Via negação de registro para um Agente Usuário;

No primeiro deles, uma mensagem de resposta simples BYE é enviada de um usuário para outro, para indicar que um usuário deseja terminar a sessão. Para tal, o invasor precisa antes capturar os pacotes de um dos Agentes Usuários, preferencialmente desde uma mensagem INVITE, e obter especificamente o Call-ID e os valores; só assim, o BYE pode ser criado.

No segundo ataque de negação dos serviços, o ataque é feito associando um Agente usuário legítimo à um endereço de IP falso ou não-existente.

Já no último tipo a ser relatado diz respeito à uma remoção do Usuário Agente do servidor SIP Proxy ou SIP Registrar. Como não existe uma mensagem "UNREGISTER", o invasor pode atingir seu objetivo alterando o tempo de expiração da sessão, que tipicamente é 3600 segundos, para zero segundo. Este processo pode ser feito repetidas vezes, pois o SIP sempre tentará se registrar novamente.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.2 VIA PROTOCOLO DE CONEXÃO H.323

A seguir, lista dos ataques que são estudados:

- Enumeração do nome de usuário;
- Recuperação de senha;
- Ataque por repetição;
- Clone do terminal;

- Ataques por saltos E.164;
- Negação de Serviço (*Denial of Service, DoS);*

2.2.1 Enumeração do nome de usuário

O atacante simplesmente captura os pacotes de conexão de um terminal H.323 e obtém o nome de usuário (*H.225 usernames*) em texto claro. A partir deste dado, outros tipos de ataques podem ser tentados, como por exemplo os de força-bruta.

Referência: PORTER, Thomas et al. **Practical VoIP Security.** Rockland, MA: Syngress Publishing Inc, 2006.

2.2.2 Recuperação de senha

Utilizando o método de enumeração do nome do usuário, um próximo passo que pode ser pensado é a recuperação de senha deste. No H.225, responsável pela informação do nome de usuário, a senha é codificada pelo padrão ASN-1, embutida na própria informação do nome de usuário. Esta informação, por sua vez, é criptografada pelo algoritmo MD5. Entretanto, esta senha pode ser quebrada por um ataque de dicionário, feito offline, pois a senha geralmente é o número do terminal, contendo entre 3 e 6 dígitos.

Referência: ROSENBERG, J. et al. **RFC 3261: SIP:** Session Initiation Protocol. IETF, 2002.

2.2.3 Ataque por repetição

O ataque por repetição pode ser feito graças a possibilidade de reenviar de uma fonte diferente, o mesmo valor de criptografia (*hash*), num password de valor equivalente, e este ser autenticado com sucesso. Por exemplo, o atacante, ao capturar o valor *hash* de uma criptografia MD5, pode utilizar tal dado para replicar tal valor e também obter a autenticação. Quanto menor for a variação de tempo do hash do MD5, mais propenso a este ataque a rede VoIP estará.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

2.2.4 Clone do terminal

O plano de numeração internacional E.164 está por trás de cada terminal H.323 e isto ajuda a identificar tal numa rede. O padrão de numeração pode ser clonado, e tal dado, um terminal de um invasor pode tomar tal valor e se registrar num *gatekeeper*. Caso o planejamento da rede VoIP preveja um controle de não duplicação do E.164, o intruso é obrigado a fazer um ataque *DoS* para o terminal com o E.164 original. Do contrário, não é necessário esta ação secundária.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.2.5 Ataques por saltos E.164

Partindo do princípio que os terminais podem ser clonados graças ao plano de numeração internacional E.164, o invasor pode dar saltos nos níveis internos de segurança, como por exemplo, ter permissão a fazer ligações para quaisquer destinos dentro de uma central telefônica, como por exemplo, ligações de saída internacionais, gerando altos custos imprevisíveis. Outro tipo de salto que pode ser dado é a nível de rede: uma vez que o intruso já está na rede, ele pode tentar trafegar através das VLANs criadas para VoIP, caso estas não tenham qualquer tipo de proteção, e enviar por exemplo, pacotes de loop infinito de conexão para os demais terminais, ocasionando a indisponibilidade permanente destes, até alguma ação de correção.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.2.6 Negação de Serviço (*Denial of Service, DoS)*

São comuns 4 tipos de ataques de negação de serviço:

- Via NTP;
- Via UDP (rejeição de registro H.225);
- Via pacotes não-alcançáveis de terminais;
- Via H.225 nonStandard Message;

Na primeira variável, o protocolo NTP é utilizado pelo H.323 para criar a sequência de criptografia do MD5. Quando o NTP é atacado, o MD5 não pode ser gerado, causando assim a perda de pacotes de conexão e, até mesmo, a incapacidade de estabelecimento de uma comunicação.

O próximo ataque de negação de serviço é o de rejeição de registro via H.225. Para o invasor, basta enviar um pacote "*UDP Registration Reject*", que o terminal tem imediatamente terminada a sua sessão com o gatekeeper.

O terceiro ataque de negação de serviços, é o de sinalização de pacotes não-alcançáveis entre os terminais. Isto é feito repetindo uma cópia de um pacote de ICMP *Unreachable* (não-encontrável) de um dos endereços de host. Este ataque chega a desconectar uma chamada já estabelecida.

O último tipo de ataque de negação de serviços, chamado de H.225 nonStandardMessage. Vários pacotes que fogem dos padrões do protocolo H.225, são enviados, com os objetivos de sobrecarregar e derrubar o sistema.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.3 VIA PROTOCOLO DE TRÁFEGO DE VOZ RTP

O principal protocolo de transmissão de voz pela rede IP é o RTP (*Real Time Transport Protocol*). Os ataques à esta parte da comunicação são muito frequentes, principalmente quando o invasor tem a pretensão de obter dados sigilosos. O fluxo de voz pode sofrer três tipos de ataque, conforme a seguir:

- Escuta passiva;

- Escuta ativa;
- Negação de serviços;

2.3.1 Escuta passiva

O primeiro tipo, se baseia que o pacote RTP em texto claro pode ser capturado pela internet, assim como o telnet, o HTTP e o FTP. Porém, capturando apenas poucos pacotes de RTP não darão o resultado desejado, pois toda a conversa precisa ser capturada, para que os dados tenham sentido para o invasor. Os softwares "*Cain & Abel*" e "*WireShark*" podem ser utilizados para capturar facilmente o tráfego de voz, ordenando os pacotes RTP e salvando eles num arquivo *.wav*. Estes ataques podem ser feitos em tempo real, com as ferramentas citadas acima, para que o chamador consiga capturar a voz quando ela for transmitida pelos interlocutores.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.3.2 Escuta ativa

O ataque passivo utiliza também ferramentas conhecidas para a captura de pacotes, porém executa ataques contra conversas ativas, como por exemplo:

- a inserção de áudio (através da captura do SSRC (*Synchronisation Source* – Fonte de Sincronismo), que nada mais é do que a informação da fonte da sinalização);
- ataques por rearranjo de informações (com o invasor inserindo informações de tempo máximo de conversação e de sequência numérica maiores, em relação aos tempos que os da conversa vigente).

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

2.3.3 Negação de serviços

Já os ataques por negação de serviços ocorrem no tráfego RTP, assim como nos ataques a protocolos de sessão, apesar de serem mais difíceis de executar. Existem dois tipos, são eles:

- Inundação de mensagens;
- Encerramento de sessão (RTCP BYE);

A inundação de mensagens é a simples injeção de uma quantidade enorme de pacotes RTP, de forma que a quantidade de tempo para analisar os pacotes de uma sessão após o aceite do número SSRC fique muito grande, causando o atraso dos pacotes de voz, ou até mesmo a interrupção destes, causando assim um ataque de DoS.

O RTCP BYE é a manipulação do protocolo de controle do RTP, chamado de RTCP, para que este possua uma mensagem de desconexão BYE, indicando que ao menos um dos terminais finalizou a sessão RTP e, portanto, não enviará mais voz. Para tal, o invasor necessita conhecer os endereços de origem e destino, a porta utilizada e o SSRC.

Referência: ROSENBERG, J. et al. **RFC 3261:** SIP: Session Initiation Protocol. IETF, 2002.

2.4 VIA INFRAESTRUTURA

Além dos ataques via protocolos de conexão e transmissão, existem aqueles que utilizam a infraestrutura existente para possibilitar a rede convergente. Estas estruturas envolvem aspectos de softwares e hardwares de redes IP em geral, telefones físicos e servidores.

2.4.1 Captura do tráfego de estrutura VoIP utilizando software de captura de pacotes

Para assegurar que as redes VoIP não serão invadidas por tráfego de rede comum, são utilizadas VLANs separadas exclusivamente para este tipo de tráfego. Estas VLANs muitas vezes são determinadas pelas portas físicas nas quais serão conectados os cabos de rede dos *hardphones* IPs. Porém, caso um invasor queira retirar o cabo de rede de tal ponto físico, conectar o seu computador e começar a capturar o tráfego da(s) VLAN(s) de VoIP, é possível.

Para não levantar suspeitas, o invasor mais bem preparado pode ter consigo um hub, conectá-lo à porta física da VLAN de VoIP, e na sequência, conectar o aparelho IP e o seu computador no hub.

Há ainda a possibilidade do telefone IP oferecer a possibilidade de mini-switch, isto é, oferecer uma porta de rede para a conexão de dispositivos não-VoIP, como por exemplo, o computador do usuário. Caso não seja programado no telefone a separação do tráfego de telefonia, do tráfego de dados, o intruso pode conectar o seu computador diretamente no telefone IP, invadindo assim não somente o usuário do terminal, mas também toda a VLAN de VoIP à qual ele pertence.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.4.2 Ataque via terminais IP

Terminais dos fabricantes Cisco, Siemens, Avaya e Polycom são os líderes mundiais de mercado, e todos estes disponibilizam os seus parâmetros de segurança. Entretanto, ataques como o envio do arquivo danificado de configuração do aparelho, causando seu mal funcionamento, ou mesmo desconexão do *gatekeeper*, é simples, porém eficiente.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.4.3 Explorando as fraquezas do SNMP

Assim como muitos dispositivos de redes IP, os terminais VoIP geralmente possuem suporte ao protocolo SNMP (*Simple Network Management Protocol* – Protocolo Simples de Gerenciamento de Redes). A versão mais popular do SNMP é a 1; e também é a mais insegura. Ela transmite as informações de gerenciamento da rede em texto claro pela rede, isto é, sem qualquer criptografia. Os dados trafegados permitem ao invasor obter dados de configuração dos terminais, como por exemplo, a tabela de roteamento sobre os outros terminais IP.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.4.4 Utilizando o NMAP

O NMAP (*Network Mapper* – Mapeador de Rede) é a ferramenta mais utilizada para se obter dados das portas numa rede IP. Se aplicado numa rede VoIP, o invasor pode descobrir as portas e serviços vulneráveis que estão habilitados, como por exemplo, as portas 21 (TCP), 23 (Telnet) e 80 (HTTP). Estes serviços (e suas respectivas portas) podem expor as senhas de administração do sistema em texto claro, podendo o intruso fazer um ataque do tipo *Man-in-the-middle*.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.4.5 Envenenamento de DNS

A gravação do endereço de DNS é usada para armazenar as informações de domínio ou *hostname*, para um endereço IP. O protocolo SIP, por exemplo, utiliza estes dados para encontrar os servidores proxies e registrars.

O objetivo de um invasor, ao envenenar o DNS, é substituir os dados originais de DNS, por dados que redirecionem para a sua rede.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

2.4.6 Burlando a tabela ARP

A tabela ARP é o método do IPv4 que relaciona endereços de rede (camada 3 OSI) com o MAC Address (camada 2 OSI). Fazendo uso de ferramentas de mercado, um intruso pode burlar um dispositivo na rede, enviando informações ARP não solicitadas para o endereço alvo. Estas informações contém o endereço MAC do dispositivo existente na rede, porém associado à um endereço IP externo (do intruso).

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

3 MECANISMOS DE SEGURANÇA MAIS COMUNS

Neste capítulo, serão estudados os mecanismos mais utilizados para combater possíveis ataques à rede VoIP. As principais formas são:

- Reforçando a segurança via protocolo de conexão SIP;
- Reforçando a segurança via protocolo de conexão H.323;
- Reforçando a segurança via protocolo de transmissão RTP;
- Segregando o tráfego lógico da rede;
- Reforçando a segurança na infraestrutura;
- Confirmando a autenticidade do usuário;
- VPN (*Virtual Private Network* - Rede Virtual Privada);
- *Firewall*;
- STUN (*Simple Traversal of UDP through NAT* – UDP Transversal Simples pelo NAT*)*;
- SBC (*Session Boarder Controller* – Controle de Sessão de Borda);

Todo estudo de segurança de redes IP parte do princípio que deve-se garantir três parâmetros: confiabilidade, integridade e disponibilidade dos dados trafegados. É visando estes que os tópicos a seguir estão organizados.

3.1 REFORÇANDO A SEGURANÇA VIA PROTOCOLO DE CONEXÃO SIP

O SIP sobre os protocolos SSLv3 ou TLSv1 - também chamado de SIPS (*SIP Security*) - é o principal método de proteção para o protocolo de conexão mais popular da atualidade de possíveis ataques. O TLS e o SSL podem encriptar a sessão desde um Agente Usuário (UAS), até um servidor SIP Proxy; além disso, este servidor pode enviar comandos para encriptar os próximos saltos, objetivando o sigilo dos dados de voz até o seu destino final.

Quando é utilizado o TLS no SIPS, o processo é muito similar ao do HTTP. A troca de certificados entre os pontos da comunicação, bem como o intercâmbio chaves de sessão, são processos comuns.

Os passos do processo de troca de informações do SIPS podem ser vistos a seguir:

1. O Agente Usuário envia uma requisição de sessão com TLS ao servidor SIP proxy.
2. O servidor SIP Proxy responde com um certificado público.
3. O Agente Usuário valida o certificado recebido do servidor SIP Proxy, utilizando uma sequência raíz.
4. O processo de intercâmbio das chaves de sessão entre o Agente usuário e o servidor SIP Proxy é feito, a fim de encriptar e desencriptar as informações da sessão SIP.
5. O servidor SIP Proxy contata o próximo salto, para atingir o próximo servidor SIP Proxy, ou o próximo Agente Usuário, e negocia a sessão TLS pelos próximos saltos, até atingir o objetivo final, fechando assim uma comunicação fim-a-fim utilizando o SIPS.

Referência: ROSENBERG, J. et al. **RFC 3261:** SIP: Session Initiation Protocol. IETF, 2002.

3.2 REFORÇANDO A SEGURANÇA VIA PROTOCOLO DE CONEXÃO H.323

Como se sabe, o protocolo de conexão H.323 é um conjunto de protocolos, cada qual com a sua função específica, em busca de garantir uma conectividade satisfatória. O responsável por garantir a segurança da conexão é o H.235. Ele é baseado no fato de que a maior ameaça à uma rede VoIP é a escuta silenciosa feita por um invasor. Os ataques *DoS* não são prevenidos pelo H.235.

Os métodos de criptografia mais comuns são o DES (*Data Encryption Standard* – Criptografia Padrão de Dados), o 3DES (*Triple Data Encryption Standard* – Criptografia Padrão de Dados Tripla) e o AES (*Advanced Encryption Standard* – Criptografia Padrão Avançada). O TLS (*Transport Layer Security* – Segurança na Camada de Transporte) e o IPSec (*IP Security* – Segurança IP) são os protocolos responsáveis pela segurança nas camadas 4 e 3, respectivamente. O IPSec tem um importante papel na criptografia dos dados de cabeçalho do conjunto H.323. Já o TLS criptografa somente os pacotes úteis, mantendo assim o endereçamento IP.

São listadas abaixo as interações do H.235 com os protocolos mais importantes do H.323:

- H.245: A sinalização de chamada do H.245 pode ser assegurada pelo TLS. Os usuários devem ser autenticados durante o início de uma conexão segura de H.245, e trocar certificados neste canal.
- H.225.0/Q.931: O TLS ou o IPSec podem assegurar qualquer troca de mensagem (Q.931) do protocolo H.225.0.
- H.225.0/RAS: Durante a fase de registro do RAS, o terminal e o gatekeeper podem trocar informações sobre as políticas de segurança para definir os métodos a serem utilizados no início de uma sessão.
- RTP/RTCP: As mensagens do protocolo H.245 são utilizadas para prover segurança não à conexão do H.323 e sim, à transmissão feita via RTP e RTCP. Esta é feita utilizando os protocolos de criptografia DES, 3DES e AES.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

3.3 REFORÇANDO A SEGURANÇA VIA PROTOCOLO DE TRANSMISSÃO RTP

O RTP seguro, também conhecido pela sigla SRTP, definido pela RFC 3711, é o protocolo que visa a proteção dos dados trafegados numa comunicação VoIP (os protocolos vistos nos subcapítulos 3.1 e 3.2 buscam a segurança apenas na autenticação da conexão).

O SRTP trabalha criptografando os dados de RTP, que normalmente são transmitidos em texto claro. O cabeçalho do RTP não é criptografado, porque todos os pontos de conexão VoIP da rede precisam saber dos caminhos almejados. Porém, para prover autenticação e integridade para o cabeçalho do RTP, é utilizada uma função HMAC-SHA1. Para criptografia do tráfego útil, o SRTP utiliza a criptografia oferecida pelo AES.

O SRTP pode dar uma falsa sensação de segurança. Isto porque, se o protocolo de conexão (SIP ou H.323) estiver com uma conexão sem tunelamento TLS, por exemplo, a chave mestre do SRTP pode ser capturada nos pacotes dos protocolos de conexão. Ou seja, sempre utilize o SRTP em conjunto com uma criptografia do protocolo de conexão.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

3.4 SEGREGANDO O TRÁFEGO LÓGICO DA REDE

A separação lógica do tráfego de voz e do tráfego de dados é altamente recomendada, para que evitar que problemas na rede de dados afetem a rede de voz, e vice -versa. As VLANs podem organizar uma rede por funções de dispositivos, tipos de serviços, acessos dos usuários, velocidade de conexão requisitada, e outros critérios. A separação dos domínios de broadcast trazidos com as VLANs reduzem o tráfego concentrado, objetivando uma rede mais balanceada. Elas trabalham na camada 2 do modelo OSI e a sua implementação mais comum é através do protocolo 802.1q, da IEEE.

Num ambiente VoIP, com *softphones*, garantir que os *malwares* encontrados nos computadores que possuam tal aplicativo de telefonia VoIP não invadirão a VLAN, é tarefa das mais difíceis. Sendo assim, a VLAN por si só não é um mecanismo de segurança eficiente, devendo toda a rede, tanto de voz, quanto de dados, estar protegida de ataques externos que possam estar implícitos.

Referência: ODOM, Wendell. **CCENT/CCNA ICND 2.** Rio de Janeiro: Alta Books editora, 2008.

3.5 REFORÇANDO A SEGURANÇA NA INFRAESTRUTURA

Para reforçar a segurança na infraestrutura de rede IP existente, é importante definir antes de tudo as políticas de segurança e os processos a serem utilizados. Esses devem ser:

1. Fáceis de compreender já na primeira leitura.
2. Textos curtos e amigáveis.
3. Fáceis de assimilar com os responsáveis.
4. Prático.
5. Definir os objetivos, e não os mecanismos para atingí-los.

Porém, não só definir os objetivos para a segurança será suficiente: estes devem ser colocados em prática. Existem diretrizes para a segurança em redes, conforme abaixo:

- Segurança física: ambiente bem protegido, permitindo acesso apenas às pessoas que trabalham diretamente com os parâmetros da rede. Ela também diz respeito à disponibilidade de acesso nos dispositivos (por exemplo, liberação de entrada USB para pendrive); hábitos dos usuários no local (p. ex.: beber, fumar, comer); e local

seguro de catástrofes naturais (para este, se necessário, deve ser garantida a redundância do sistema em outro local, de preferência à uma distância segura).

- Protegendo os servidores: desabilite qualquer serviço que não esteja utilizando e apague aqueles que nunca utilizará. Isto porque os invasores utilizam serviços e programas que estão parados nos servidores, para invadir uma rede. Esta estratégia é utilizada pois sabe-se que um serviço ou programa não utilizado tem uma probabilidade muito maior de não estar sendo monitorado pelo administrador da rede.
- Serviços de suporte: para que o VoIP tenha sucesso em todas as suas etapas, ele precisa do apoio de alguns serviços, como por exemplo, DNS, DHCP, HTTPS, SNMP, SSH, NTP, TFTP, entre outros. O recomendado é que os serviços indicados sejam dedicados ao VoIP (embora isto seja muito difícil num ambiente prático). Estes serviços, no ambiente ideal de segurança, devem conter proteção de firewalls, IDS, IPS, ou todos estes combinados.
- Gerenciamento centralizado da rede: um dos grandes benefícios do VoIP é poder gerenciá-lo numa rede IP, com as mesmas facilidades que o tráfego de dados é gerenciado. Algumas ferramentas precisam ser adaptadas para suportar o monitoramento do tráfego VoIP.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

3.6 CONFIRMANDO A AUTENTICIDADE DO USUÁRIO

Parte-se do princípio que a autenticação é uma medida de confiabilidade. Ela estabelece as identidades dos dispositivos e usuários de acordo com o nível de segurança desejado. A autorização, por sua vez, estabelece os tipos de aplicação que podem ser utilizados numa rede, e os níveis de acesso dos usuários para a utilização destas aplicações.

Algumas medidas simples podem ser tomadas, como a verificação do usuário através do método do resumo da autenticação do HTTP (*HTTP Digest Authentication*) e lista de filtros de MAC Address. Entretanto, soluções simples como estas podem facilmente ser corrompidas pelo invasor. Para uma solução VoIP corporativa, soluções como o 802.1x/EAP, certificados de infraestrutura, ou então uma combinação de tais soluções, é o mais indicado.

Em ambientes H.323, a base da autenticação é definida pelos terminais, para a conexão com os seus respectivos gateways ou gatekeepers. Com tal, é possível afirmar que o gatekeeper conectará o terminal H.323 com o número discado, e não com qualquer outro número que possa ser invasor.

Em ambientes SIP, ao contrário do que acontece nos ambientes H.323, não existem regras pré-definidas para a segurança. Todavia, os desenvolvedores utilizam os mecanismos mais comuns para o HTTP, como por exemplo, o S/MIME, o TLS, o IPSEC (todos estes, garantem integridade dos dados, confiabilidade e autenticação, esta via PKI) e o HTTP 1.1 Digest, que não garante a integridade dos dados, nem confiabilidade, e utiliza uma chave pré-compartilhada para a autenticação (que é fácil de ser quebrada).

3.6.1 802.1x/EAP

O padrão 802.1x é baseado na autenticação do usuário primeiramente num servidor, que pode ser do tipo RADIUS (*Remote Authentication Dial In User Service*, se baseia nos princípios AAA, sendo a sigla, em português: Autenticação, Autorização e Contabilidade), para em seguida ter a porta de conexão preterida liberada pela LAN. O EAP provê um quadro no cabeçalho, que oferece a possibilidade de múltiplos métodos de autenticação no servidor do 802.1x, como por exemplo, os Certificados Digitais e a autenticação por chave pública.

Sendo assim, o 802.1x/EAP é utilizado não como um padrão sozinho, pois trabalha em conjunto com outros protocolos para prover parâmetros de autenticação (utiliza os métodos citados no parágrafo acima), bem como de criptografia (utiliza, por exemplo, o TLS ou o AES), através de um servidor que, posteriormente, indicará a LAN a permissão ou não da porta desejada.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

3.6.2 PKI

O PKI (*Public Key Infrastructure* - Infraestrutura de Chave Pública) é reconhecido por funções determinísticas, de identificação automatizada, autenticação, controle de acesso e autorização.

O principal objetivo do PKI é facilitar a utilização dos certificados X.509 para aplicações de Internet, sendo o VoIP uma destas.

Dentro da Infraestrutura de Chave Privada, o usuário é definido a partir das chaves privadas que possui. As chaves privadas são trocadas entre os usuários e, para que estes aceitem a comunicação, possuem os mesmos códigos de decriptografia para interpretar se a chave está correta. Por terem os mesmos códigos, pode-se dizer que esta troca é simétrica.

Já na Infraestrutura de Chave Pública, numa comunicação entre dois usuários, um algoritmo de chave pública do destinatário (que pode ser conhecido pela rede) é utilizado pelo emissor para criptografar uma senha. Porém, somente o destinatário detém a chave privada que pode decriptografar o texto. Pode-se fazer uma analogia entre uma fechadura e uma chave: a fechadura é pública e disponível para qualquer entidade na rede, para que com sua chave, possa tentar abrí-la; entretanto, somente a chave específica para tal fechadura conseguirá abrir. No processo PKI, a chave privada também é utilizada para assegurar, via assinatura digital (criada com a troca de sequência da mensagem), a veracidade da identidade do usuário. A chave pública, por sua vez, coloca na ordem correta a informação da identidade do usuário. A troca de chaves é assimétrica.

Relacionado ao PKI, o certificado de autorização (CA) X.509 faz uso do PKI atrelado ao seu campo de sujeito (SPKI - *Subject Public Key Infrastructure*) para transportar a chave pública e o algoritmo de criptografia (por exemplo, RSA, DSA ou Diffie-Hellman). Os campos do X.509 contém informações como as identificações do emissor e do destinatário, uma chave pública associada ao destinatário, um prazo de validade e uma assinatura; esta é adicionada aos demais campos já codificados.

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

3.6.3 Verificação de MAC address

Os telefones IP baseados em *hardware* (*hardphones*), bem como os baseado em *software* (*softphones*) possuem um MAC address associado, neste o MAC do computador no qual roda a aplicação, e naquele o do próprio hardware. Os *gatekeepers*, *gateways* e MCUs, sendo dispositivos VoIP e, portanto, de rede, também possuem MAC address. Partindo deste princípio, um gatekeeper pode ter uma lista dos MAC address que são autorizados para tentar uma conexão. Todo e qualquer MAC address que não estiver na lista, terá a sua conexão

negada pelo gatekeeper. Este método por si só, contudo, é vulnerável à ataques de dispositivos que clonaram o MAC address de um dispositivo cadastrado na lista de permissão do gatekeeper.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

3.7 VPN

Para garantir uma comunicação segura, através de rede não segura - como grande exemplo desta, a rede WAN - sem a necessidade de um link dedicado ponto-a-ponto de alto custo, são utilizadas as VPNs (*Virtual Private Networks* - Redes Virtuais Privadas). Para os dispositivos e usuários interconectados via VPN, suas conexões com as redes LAN são transparente, com acesso total à rede (dentro dos limites de política de segurança das LANs que estão acessando). Do ponto de vista de usuários móveis, as VPNs trazem uma maior economia, escalabilidade e flexibilidade, pois torna possível o acesso às redes privadas, onde quer que estejam. Segundo o órgão de pesquisa Forrester Research, quando se cria uma VPN, a redução dos custos, em geral, pode ser maior que 60%.

Existem dois tipos de VPN: Gateway-to gateway e client-to-gateway. No primeiro, num ambiente VoIP, pode ser pensado como duas ou mais localidades, com seus respectivos gatekeepers (por exemplo, PABX), interligadas via VPN. Já no segundo, também com foco na voz sobre IP, um ambiente prático é o usuário ter um softphone no seu smartphone ou notebook - utilizando a rede WAN - autenticado num gatekeeper (mais uma vez como exemplo, um PABX) conectado à uma LAN.

Como um dos seus pilares, a segurança na VPN deve ser garantida; afinal, os dados trafegaram, na maioria dos casos, pela WAN, que é uma rede aberta e, portanto, insegura. Para tal, os dois principais fundamentos são a criptografia e o tunelamento.

A criptografia tem o objetivo de garantir a integridade, o sigilo e a autenticidade. A criptografia pode fazer uso dos seguintes protocolos:

- L2TP - protocolo de camada 2;
- PPTP - protocolo de camada 2;
- IPSec - protocolo de camada 3;

Os protocolos de camada 2 fazem uso apenas da autenticação, enquanto o IPSec, da camada 3, faz uso da autenticação, da integridade e do sigilo. O IPSec se mostra a melhor escolha para VoIP, pois garante as seguintes funcionalidades:

- O *Authentication Header* - AH, que fornece a integridade dos pacotes e a garantia de sua origem;
- O *Encapsulation Security Payload* - ESP, que fornece o sigilo dos dados trafegados;
- O *Internet Key Exchange* - IKE, que permite a negociação das chaves, entre os dispositivos a serem conectados, de modo seguro.

Já o conceito de tunelamento permite que os usuários tenham total nível de autorização à uma LAN, mesmo estando numa WAN, pois os dados trafegados nesta se encontraram preservados num túnel, no qual o invasor não terá acesso, devido aos seguintes protocolos de segurança:

- L2TP - protocolo de camada 2;
- PPTP - protocolo de camada 2;
- L2F - protocolo de camada 2;
- VTP - protocolo de camada 2;
- MPLS - protocolo de camada 2;
- Mobile IP - protocolo de camada 3
- IPSec - protocolo de camada 3;

Em oposição ao que ocorre na criptografia, os protocolos de camada 2 do modelo OSI levam vantagem em relação aos protocolos de camada 3, pois exigem menor esforço computacional, possuem boa compressão, fazem a codificação completa e inicializam o túnel bidirecionalmente.

Todas estas informações de codificação e tunelamento da VPN ocupam um espaço adicional do cabeçalho, e consequentemente, aumentam o overhead, exigindo maior largura de banda para a transmissão dos pacotes de voz na rede. No próximo capítulo, poderá ser interpretado um estudo sobre tal cosumo adicional de largura de banda da rede.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

3.8 FIREWALL

O firewall é um importante componente de qualquer arquitetura de segurança de rede, pois ele demarca o que é rede interna e o que é rede externa, redes confiáveis e não-confiáveis, e ainda pode ser usado para separar o que é tráfego de voz, do que é tráfego de dados. Porém, na sua implementação, é importante considerar três pontos críticos: a abertura para tráfego externo, critérios menos rigorosos sobre o tráfego não-confiável e análise dos pacotes VoIP, principalmente quando estão criptografados.

Quanto a implementação de VoIP numa rede já em funcionamento, existem dois pontos que devem ser pensados:

- A liberação de uma faixa muito grande de portas altas (>1024), pois os parâmetros de tráfego das chamadas, tráfego de mídia e controle de tráfego de mídia, utilizam portas altas, em grande quantidade e arbitrárias;
- A alteração das informações de endereços IP e portas de acordo com o tráfego VoIP, que dificulta uma análise precisa do firewall quanto a liberação ou não do fluxo em questão.

Para o protocolo de conexão H.323, pelo menos as seguintes portas são requiridas:

- Descoberta de gatekeeper: 1718 – UDP;
- Gatekeeper RAS: 1719 – UDP;
- Ajuste de sinalização da chamada via Q.931: 1720 – TCP;
- Sinalização H.245: portas entre 1024 e 65535 – TCP;
- RTP/RTCP (tráfego): portas entre 1024 e 65535 – UDP;
- Sinalização de segurança H.235: 1300 – TCP;

A conclusão é que o controle de portas para a gama de protocolos que formam o H.323 é muito complexa, pois exige que uma faixa muito grande de portas (todas acima de 1024), tanto TCP, quanto UDP estejam liberadas. Outro fator que complica tal filtro é a codificação das mensagens de sinalização e controle no padrão ASN.1.

O protocolo de conexão SIP tem como principais portas as seguintes:

- SIP: 5060 – UDP;
- SIPS: 5061 – UDP;

Estas portas estão ligadas apenas ao estabelecimento da ligação. O tráfego da voz é responsabilidade dos protocolos RTP/RTCP que, no geral, utiliza portas as portas acima de 1024; entretanto, no gatekeeper, geralmente é possível limitar a faixa de portas que protocolo o tráfego utilizará. Um bom número de portas, num gatekeeper de pequeno ou médio porte, é de 200 portas. Porém, como o protocolo SIP é baseado nas mensagens HTTP, ele também apresenta as mesmas vulnerabilidades deste protocolo.

As listas de controle de acesso (ACLs) são parâmetros dos firewalls, que trabalham na camada 3 do modelo OSI, são utilizadas para permitir ou negar determinados tipos de tráfego de saída ou entrada, de acordo com os endereços IP de origem e destino, portas de origem e destino, wildcards, e outros dados, dependendo do tipo de ACL.

Assim como as VLANs, as ACLs são ferramentas poderosas para a segregação do tráfego VoIP na rede.

Referência: NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

3.10 STUN

O STUN (*Simple Traversal of UDP through NATs* – Encaminhamento simples do tráfego UDP através do NAT) é um protocolo de arquitetura cliente-servidor designado a habilitar um terminal para descobrir o seu endereço público e o seu tipo de NAT, para que possa alcançar seu destino.

O protocolo STUN descreve um cliente habilitado numa rede privada, que pode ser encontrado por um servidor STUN público. Este informa ao cliente (terminal) qual é o seu IP e porta públicos dentro, por exemplo, de uma sessão SIP.

Abaixo, segue uma lista de endereços IP de STUN públicos:

- stun.fwdnet.netn: 69.90.168.14
- stun.fwd.orgn: 64.186.56.73
- stun01.sipphone.comn: 69.0.208.27
- stun.softjoys.comn: 69.3.254.11
- stun.voxgratia.orgn: 83.103.82.85
- stun1.vovida.orn: 128.107.250.38
- xtunnels1.xten.nen: 64.69.76.23

Referência: PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006.

3.11 SBC

Os SBCs (*Session Border Controllers* – Controladores de Borda de Sessão) tem como principal função "furar" os redirecionamentos feitos pelo NAT no firewall, possibilitando que dispositivos externos à rede LAN de um gatekeeper possam se conectar com segurança no mesmo. Isto faz com que a latência dos pacotes diminua e o dispositivo externo possa utilizar sem problemas os protocolos de conexão SIP e H.323.

Ele também é uma ferramenta poderosa de monitoramento , classificação e emissor de relatórios de tráfego.

Os fabricantes mais comuns de SBC, hoje, são a *Acme*, a *Sonus* e a *Juniper*.

Referência: DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

4 CASOS PRÁTICOS DE SEGURANÇA – LINHA DE PABX SIEMENS HIPATH 3000

Como caso prático para a implementação de alguns dos mecanismos de segurança comentados no capítulo 3, e com o objetivo de evitar os ataques mencionados no capítulo 2, foi escolhida a linha de centrais Siemens HiPath 3000, na sua última versão de software, que é a 9.0. Esta é uma central híbrida, com a capacidade de ter as tecnologias TDM e IP simultaneamente. Para ter a tecnologia IP, é necessário um módulo VoIP chamado HG (*HiPath Gateway*). O estudo discorrerá sobre os aspectos de segurança disponíveis neste módulo.

4.1 ACESSO

Os acessos possíveis podem ser divididos para quatro finalidades:

- Acesso à administração;
- Login e senha;
- Filtro de faixa de IP;
- Filtro de MAC Address;

4.1.1 Acesso à administração

Ao acessar o módulo HG via navegador, é possível discriminar quais IPs de computadores poderão acessar o módulo HG via navegador, para posterior programação. Desta forma, já evita que qualquer IP possa acessar o módulo para realizar suas configurações.

Em Explorers -> Security -> IP Administration Access, podem ser adicionados IPs de acesso, clicando com o botão direito do mouse sobre a palavra Web-Based Management e, em seguida com o botão esquerdo, em Add IP address for Administration. Após esta ação, inclua o endereço desejado, conforme a tela abaixo:

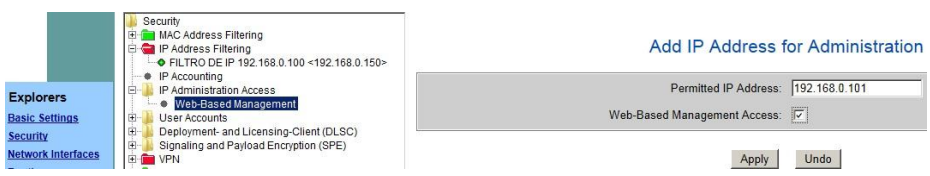


Figura 1 – IP para administração

Todavia, a regra continua desativada, conforme a seguir no campo "*Web-Based Management Access Check*". Para ativar, basta clicar com o direito do mouse em "*Web-Based Management*" e, em seguida, com o esquerdo em "*Enable Access Check*".

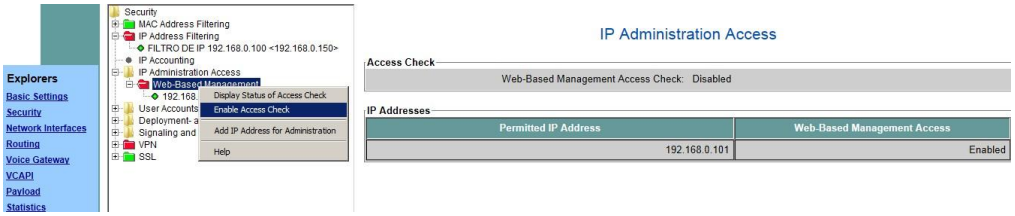


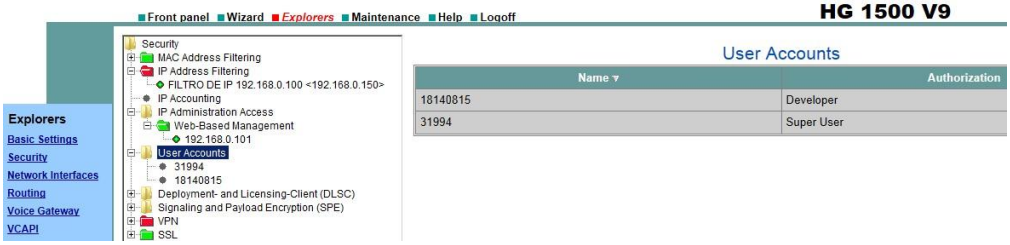
Figura 2 – Habilitando o acesso ao WBM

O resultado é que, deste momento em diante, somente os IPs ali cadastrados poderão acessar o PABX via navegador.

Figura 3 – Lista de acessos à administração do VoIP no PABX

4.1.2 Login e senha

É possível visualizar qual é o nível de acesso de cada login do sistema. Por padrão, a senha é a mesma sequência numérica do login, podendo ser alterada. O login 31994 não possui acesso às configurações avançadas de segurança, monitoramento e interligação (*Super User*). Já o login 18140815 possui acesso total (*Developer*).

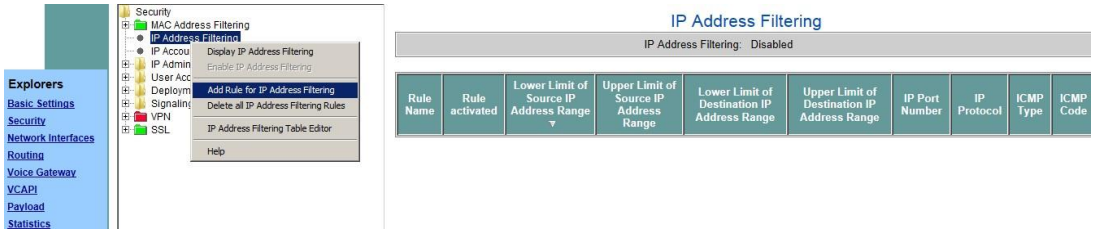


4 – Níveis de acesso para administração

4.1.3 Filtro de faixa de IP

No filtro de faixa de IP, são definidas faixas de IPs que podem enviar e receber pacotes. Este dado pode depender ainda do tipo de protocolo IP (TCP, UDP ou ICMP).

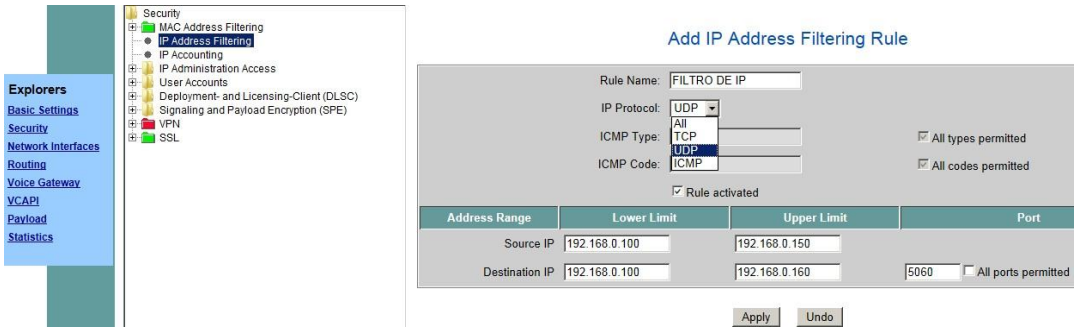
Para adicionar uma regra, basta entrar em Security, clicar com o botão direito do mouse sobre IP Address Filtering, e escolher a opção Add Rule for IP Address Filtering.



5 – Faixas de IP permitidas

O próximo passo é adicionar a faixa de IPs. Existe uma faixa que serve para os IPs de origem, isto é, os IPs que poderão enviar pacotes a partir de uma autenticação no módulo HG; para tal característica, são programados os campos *Source IP*, onde *Lower Limit* é IP com menor valor, e *Upper Limit* o IP com maior valor. Já para a faixa de IPs de destino, isto é, os IPs que poderão receber pacotes a partir de uma autenticação no módulo HG, são programados os campos *Destination IP*, onde *Lower Limit* é IP com menor valor, e *Upper Limit* o IP com maior valor.

Se no tipo de protocolo IP for selecionado, ou o protocolo TCP, ou o protocolo UDP, o campo *All ports permitted* se mostra disponível para programação, podendo então restringir para apenas uma porta o tráfego dos pacotes IP recebidos para tal faixa.

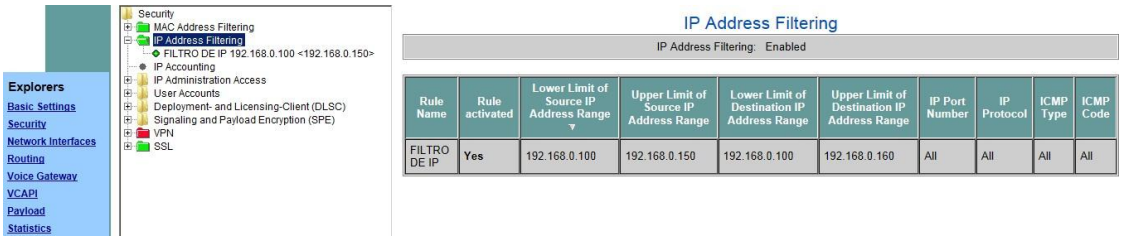


6 – Configuração das faixas de IPs de fonte e destino

Entretanto, não basta apenas configurar. É necessário ativar a regra, clicando com o botão direito do mouse sobre *IP Address Filtering*, e selecionando a opção *Enable IP Address Filtering*.

7 – Habilitação da faixa de IPs permitidas

O resultado é que a regra fica ativada, conforme pode ser visto abaixo.

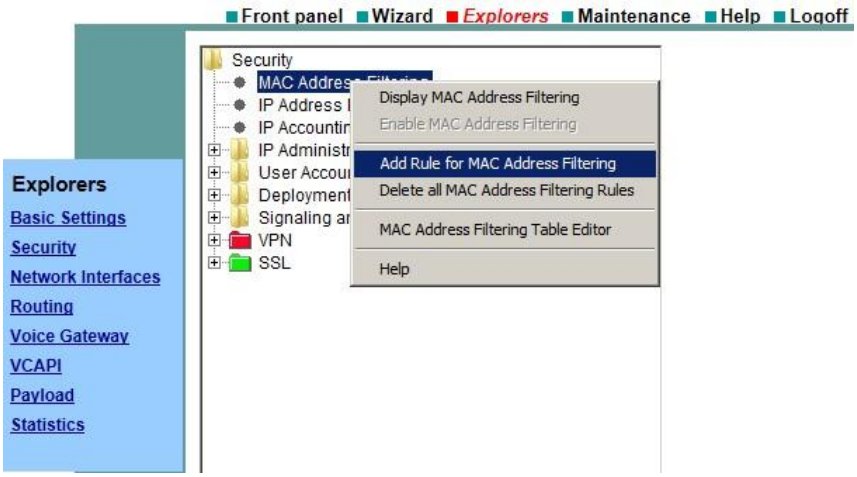


8 – Visualização dos filtros ativos

4.1.4 Filtro de MAC Address

Para garantir que realmente um programador bem intencionado, a partir de um dispositivo confiável, fará as conexões via Telnet ou SSH no *Hyperterminal*, ou via navegador, existe um filtro de MAC Address. Após a ativação da regra, somente os dispositivos cadastrados poderão realizar programações no módulo HG.

A fim de adicionar a regra, em *Security*, clica-se com o botão direito do mouse em *MAC Address Filtering*, e seleciona a opção *Add Rule for MAC Address Filtering*.

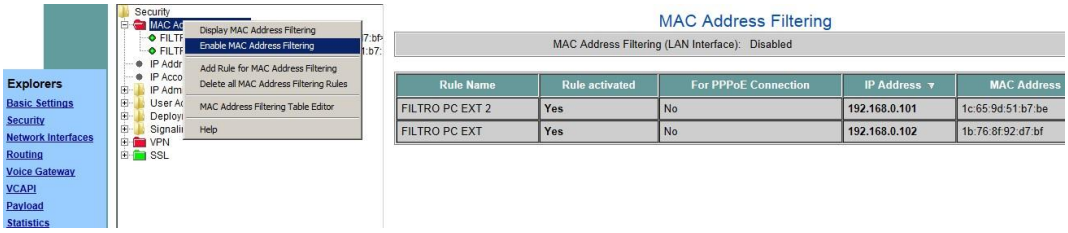


9 – Adicionando uma regra de filtro de MAC

Em *Rule Name*, coloca-se um nome sugestivo para a regra. Em *IP Address*, é associado o endereço IP que o dispositivo com o MAC relacionado acessará o gatekeeper; e em *MAC Address*, seu respectivo MAC Address. Para permitir a ativação da regra, a opção *Rule Activated* deve estar marcada.

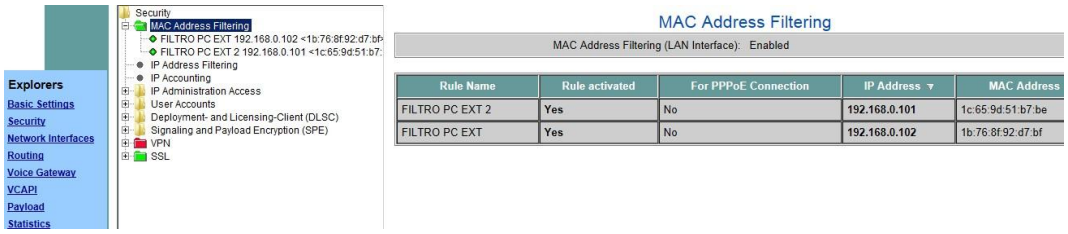
10 – Criando a regra de filtro de MAC

Da mesma forma que a regra relacionada a filtro de faixa de IP, esta regra deve ser ativada.



11 – Habilitando a regra de filtro de MAC

O resultado é a habilitação das regras no módulo VoIP.



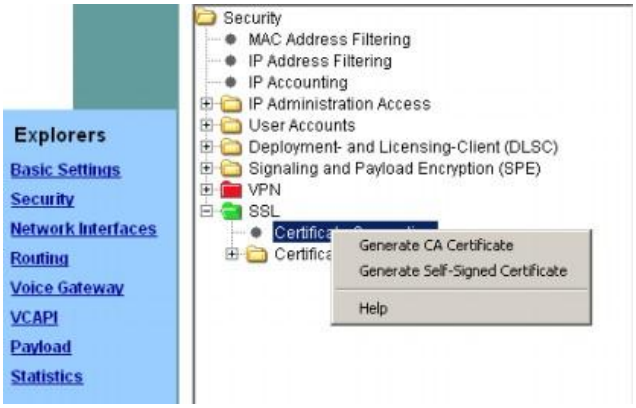
12 – Visualizando a regra de filtro de MAC

4.2 CERTIFICADOS DE AUTENTICAÇÃO

As conversas dos terminais IP que utilizam o protocolo IP proprietário da Siemens, baseado no H.323, chamado HFA (*HiPath Feature Access*), podem ser criptografadas pelo método assimétrico PKI. Para tal, conforme poderá ser conferido, são gerados Certificados de Autenticação. Este processo, para o fabricante Siemens, é chamado *Signaling and Payload Encryption* (SPE). É fundamental que todos os dispositivos estejam com a mesma data e hora.

4.2.1 Configurando o módulo HG

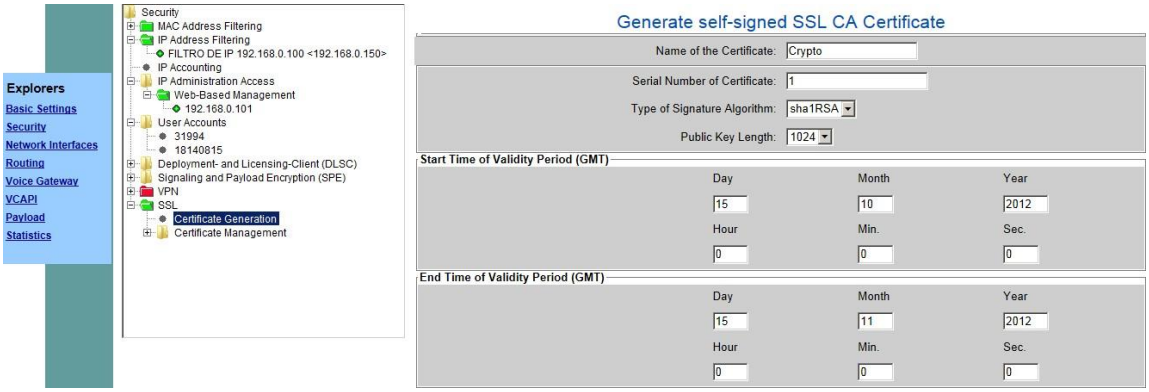
O primeiro passo é a geração do certificado. Para tal, é necessário acessar *Security*, abrir a pasta SSL, clicar com o botão direito do mouse em *Certificate Generation* e selecionar opção *Generate CA Certificate*.



13 – Criando o certificado CA

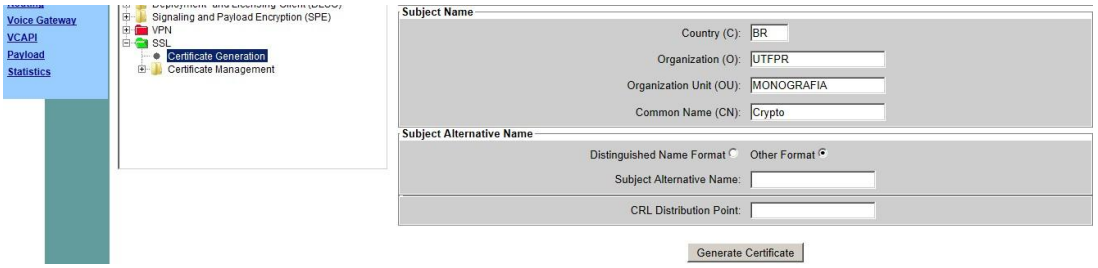
No campo *Name of the Certificate*, deve ser atribuído um nome conveniente ao certificado. Em *Serial Number of Certificate*, atribuir o valor 1; no campo *Type of Signature*

Algorithm, escolher o algoritmo de criptografia RSA para ambas todos os pontos a serem criptografados, através da opção *sha1RSA*. O tamanho da chave, em bits, é determinado pelo campo *Public Key Lenght*, e deve ser configurado com o valor 1024. Abaixo, em *Start Time of Validity Period (GMT)*, e em *End Time of Validity Period (GMT)*, é determinado o início e o término, respectivamente, da validade do certificado.



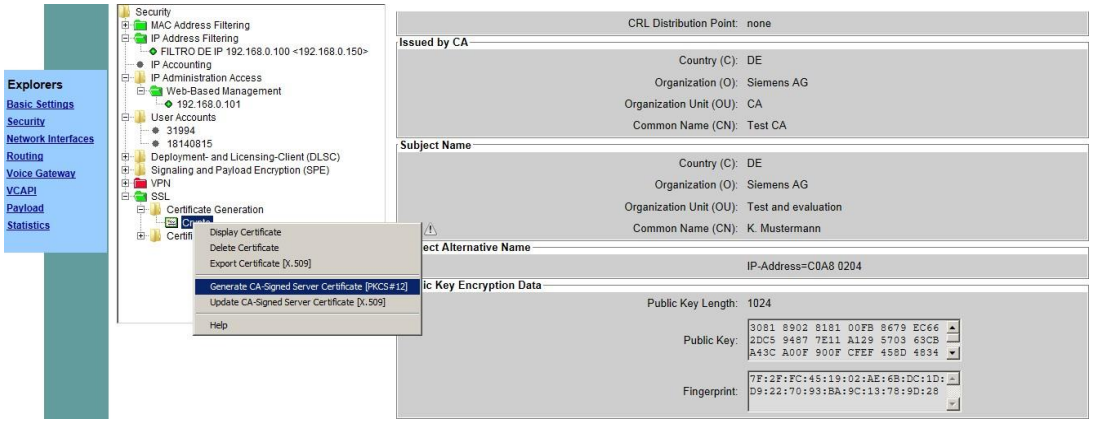
14 – Parâmetros obrigatórios para o certificado CA

A sigla do país deve ser descrita no campo *Country (C)* e, no caso do Brasil, deve ser atribuída como BR. Os demais campos são apenas informativos. Ao clicar em *Generate Certificate*, o certificado é gerado pelo módulo HG.



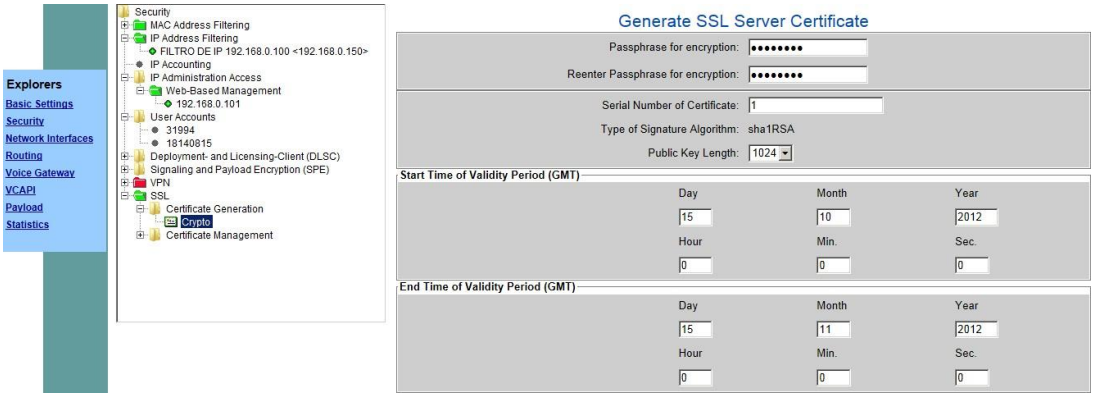
15 – Parâmetros adicionais para o certificado CA

Em seguida, é gerado o certificado para o servidor, baseado no Certificado criado no passo anterior. Para tal, basta clicar com o botão direito do mouse sobre o certificado e selecionar a opção *Generate CA-Signed Server Certificate [PKCS#12]*.



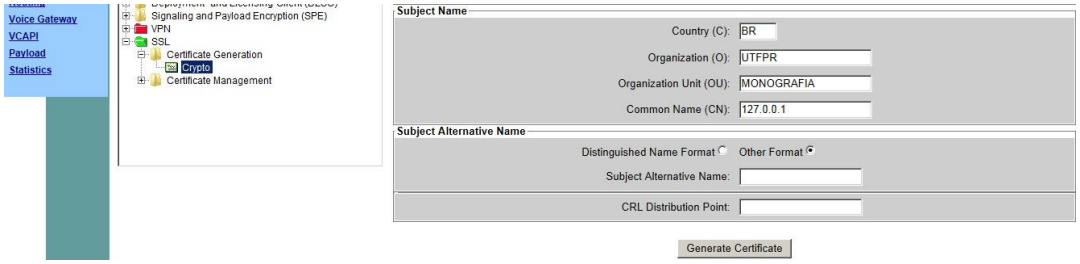
16 – Criando o certificado PKCS#12

Nos campos *Passphrase for encryption* e *Reenter Passphrase for encryption*, é atribuída a senha de criptografia. Em *Serial Number of Certificate*, o valor 1 deve ser dado. Já em *Public Key Lenght*, é dito o tamanho da chave de criptografia, que deve ser de 1024 bits. Em *Start Time of Validity Period (GMT)*, e em *End Time of Validity Period (GMT)*, é determinado o início e o término, respectivamente, da validade do certificado.



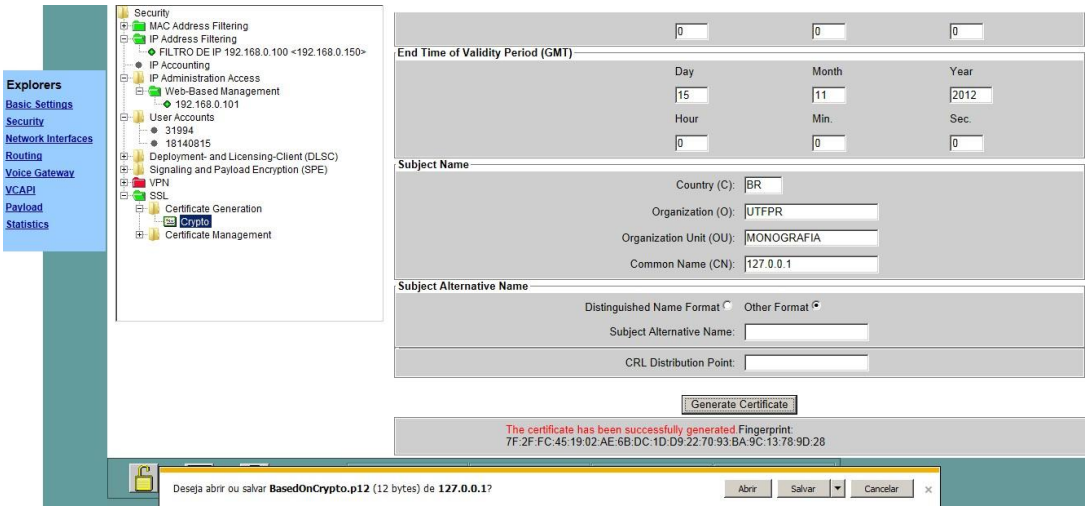
17 – Configurando o PKCS#12

O campo Country (C) deve estar com a sigla do país que, mais uma vez para o Brasil, é BR. Os campos *Organization (O)* e *Organization Unit (OU)* são apenas informativos. Porém, para a chave do servidor, o campo *Common Name* tem que ser configurado com o IP do módulo HG. Para gerar o certificado, basta clicar em *Generate Certificate*.

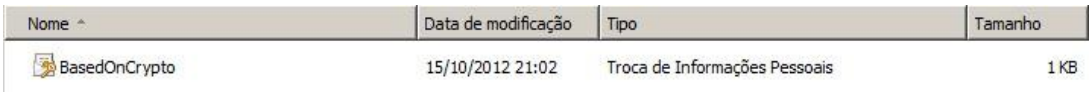


18 – Outros parâmetros do PKCS#12

Ao clicar no botão *Generate Certificate*, note que o navegador dá a opção de salvar a Criptografia e assim deve ser feito.

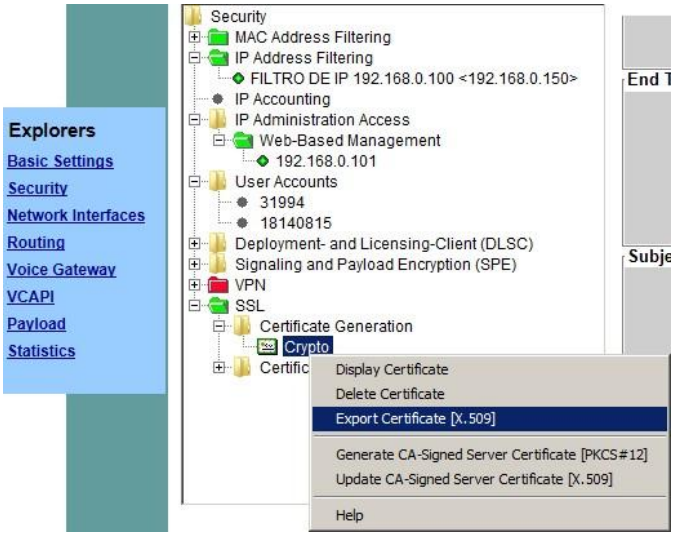


19 – Salvando as configurações do PKCS#12

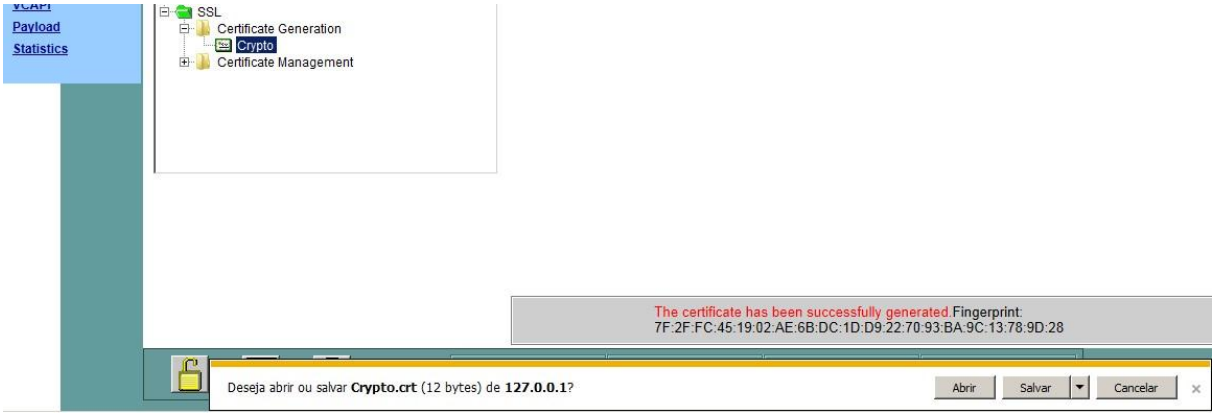


20 – Arquivo gerado sobre as configurações do PKCS#12

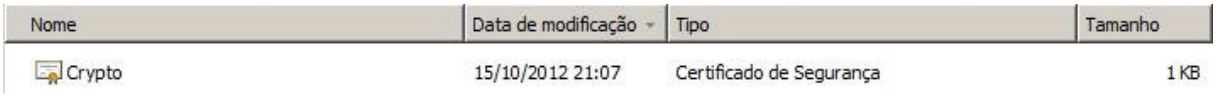
Em seguida, o certificado X.509 deve ser exportado. Para tal, é necessário clicar com o botão direito do mouse sobre o certificado e selecionar a opção *Export Certificate [X.509]*. Em seguida, o local para salvá-lo será escolhido, e o arquivo resultante poderá ser visualizado.



21 – Exportando o certificado X.509

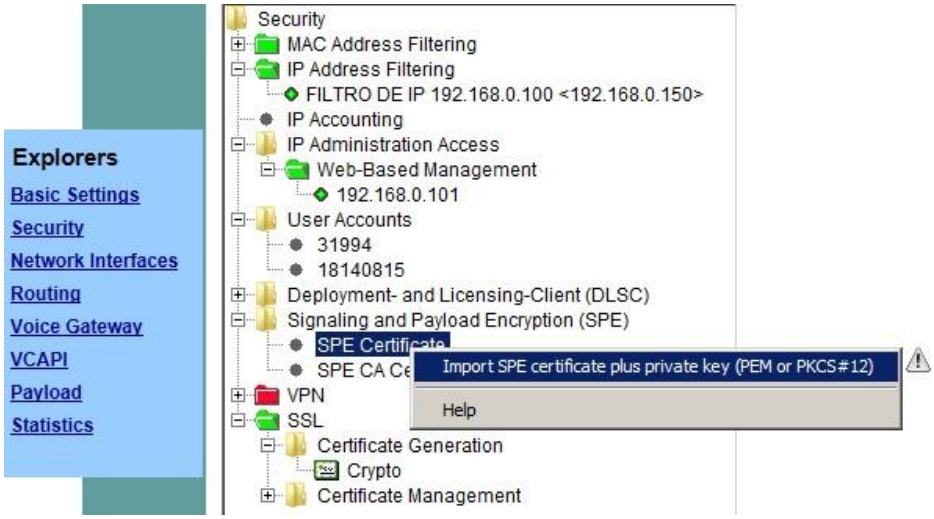


22 – Salvando o certificado X.509



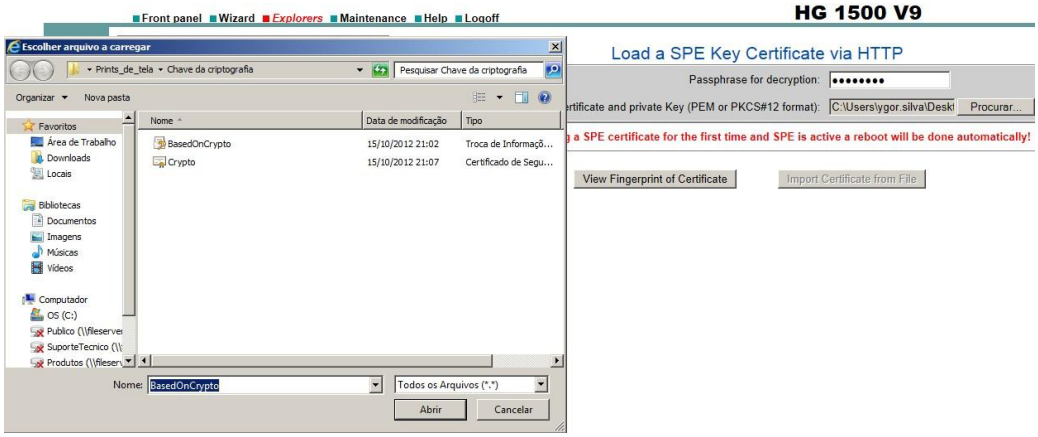
23 – Arquivo de configuração gerado pelo X.509

Na sequência, a pasta *Signaling and Payload Encryption (SPE)* deve ser aberta e, na sequência, clicar com o botão direito sobre *SPE Certificate*, escolher a opção *Import SPE certificate plus private key (PEM or PKCS#12).*



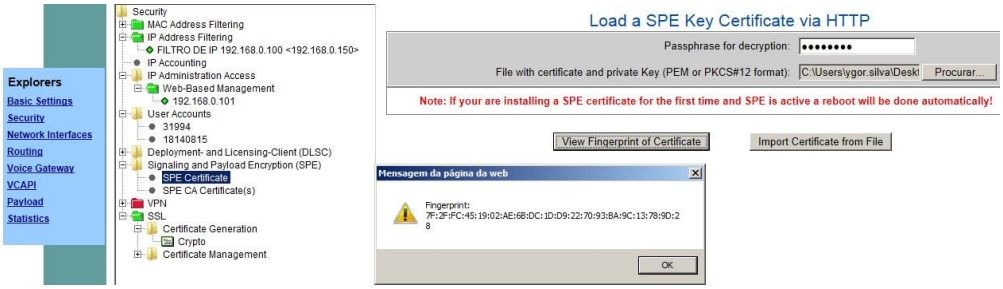
24 – Importação do certificado PKCS#12

Em *Passphrase for decryption*, deve ser colocada a mesma senha utilizada para a chave de criptografia. Na opção *File with certificate and private key (PEM or PKCS#12 format)*, inserir o caminho do primeiro arquivo de criptografia salvo no computador. Na sequência, clicar em *View Fingerprint of Certificate*.



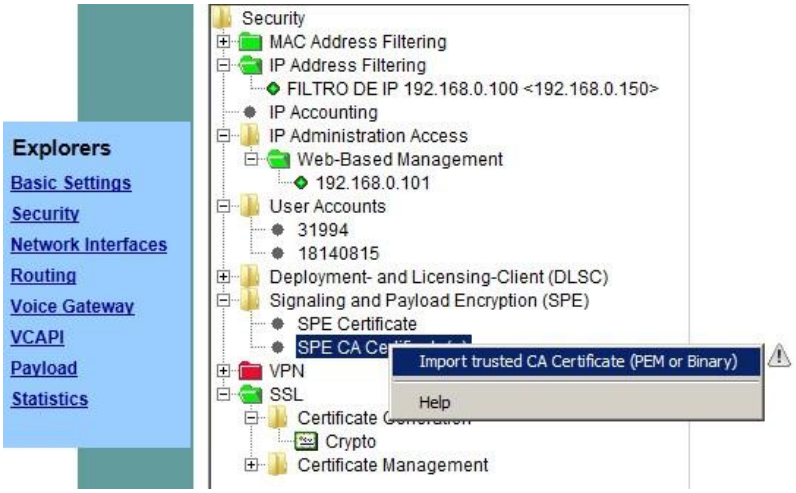
25 – Inserindo o caminho do certificado PKCS#12

Em seguida, clique em *Import Certificate from File*. O resultado do processo aparecerá na tela, apresentado com uma mensagem de *Fingerprint*.



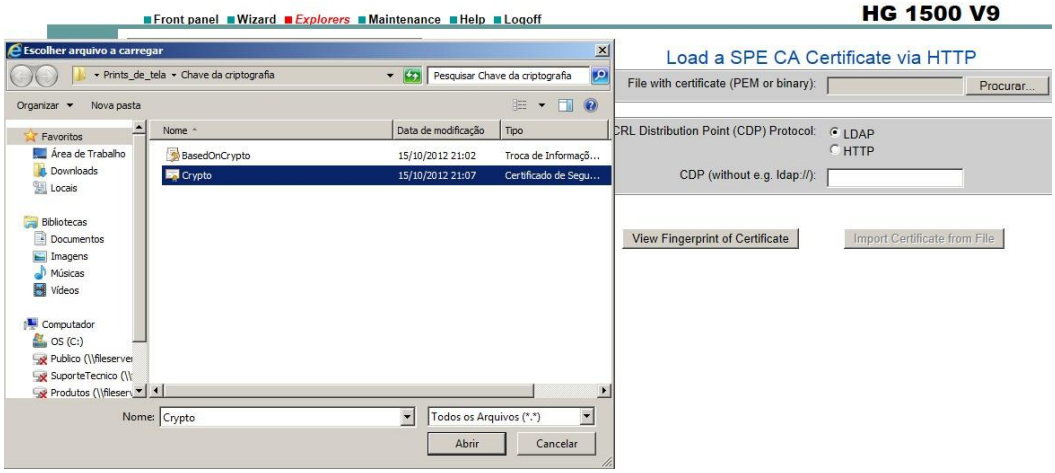
26 – Visualização da chave PKCS#12 importada

Na sequência, um processo similar deve ser feito com o certificado do servidor. Para tal, clicar com o botão direito sobre *SPE CA Certificate(s)* e selecionar a opção *Import trusted CA Certificate (PEM or Binary).*



27 – Importação do certificado CA

No campo *File with certificate (PEM or binary)*, indicar o caminho do certificado gerado para o servidor. Após, clicar em *View Fingerprint of Certificate.*



28 – Indicando o arquivo do certificado CA

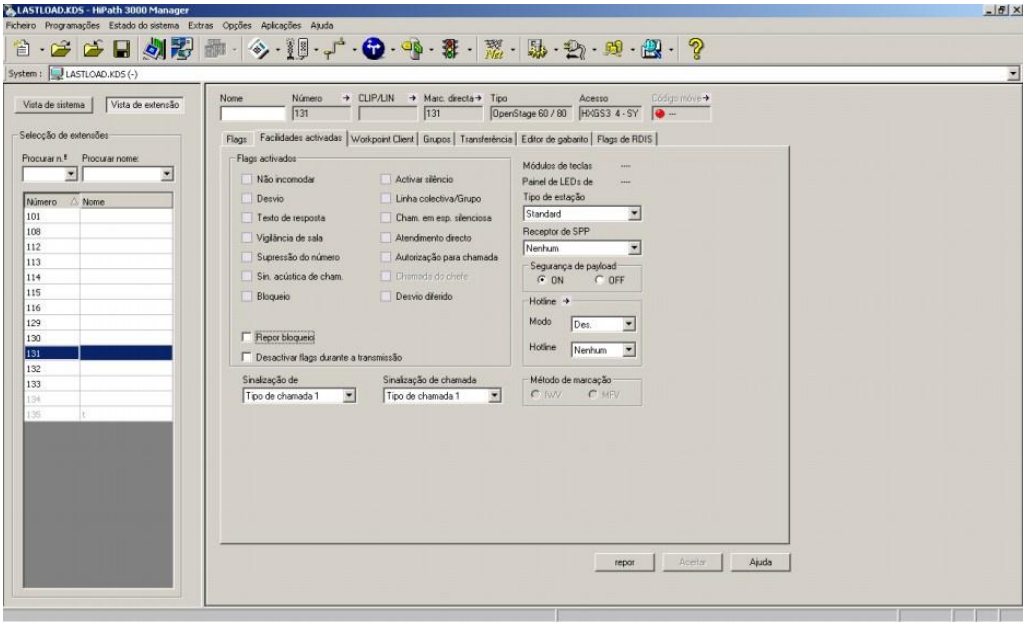
Em seguida, clique em *Import Certificate from File*. O resultado do processo aparecerá na tela, apresentado com uma mensagem de *Fingerprint*.

29 - Visualização da chave do certificado CA importado

4.2.2 Configurando o PABX

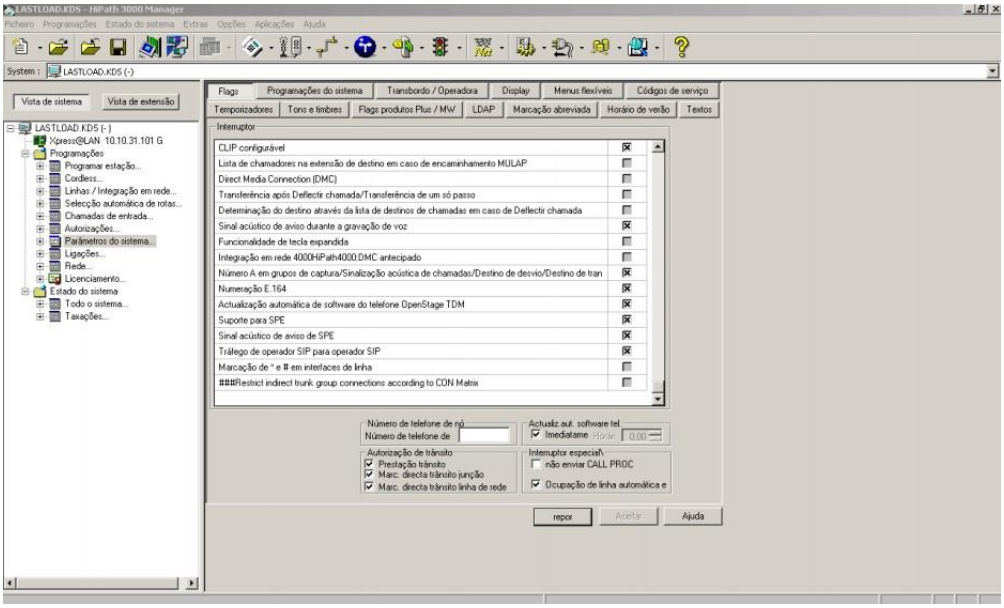
Para preparar o PABX para receber os pacotes com segurança do módulo HG, devem ser feitos os passos mostrados a seguir. O programa utilizado para tal é o Manager E.

Como dito, os terminais que utilizam o protocolo de conexão HFA podem utilizar a criptografia provida pelo processo chamado pela Siemens de SPE. Para que o ramal esteja preparado, é necessário acessar a guia Vista de extensão, subguia Facilidades activadas, selecionar os ramais que utilizarão a segurança, e marcar o campo Segurança de payload com a opção *ON*.



30 – Habilitando a segurança nos ramais IP

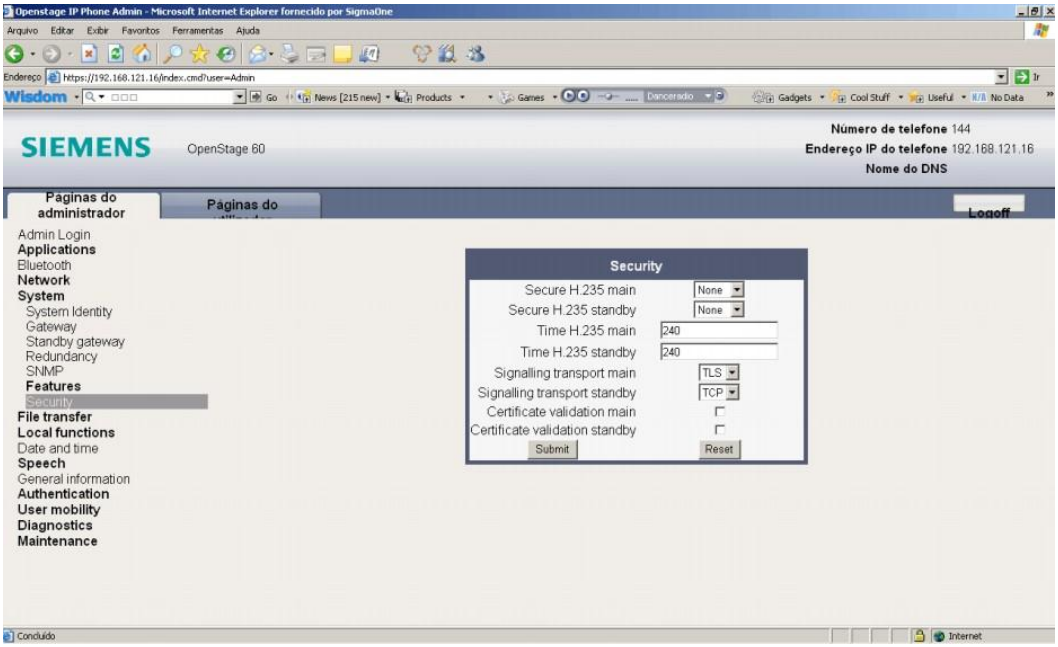
Para que o PABX Siemens HiPath 3000 esteja preparado para receber os pacotes de voz criptografados, marcar em Vista de sistema, Parâmetros do sistema, Flags, a opção Suporte para SPE.



31 – Habilitação do campo Suporte para SPE

4.2.3 Configurando o terminal

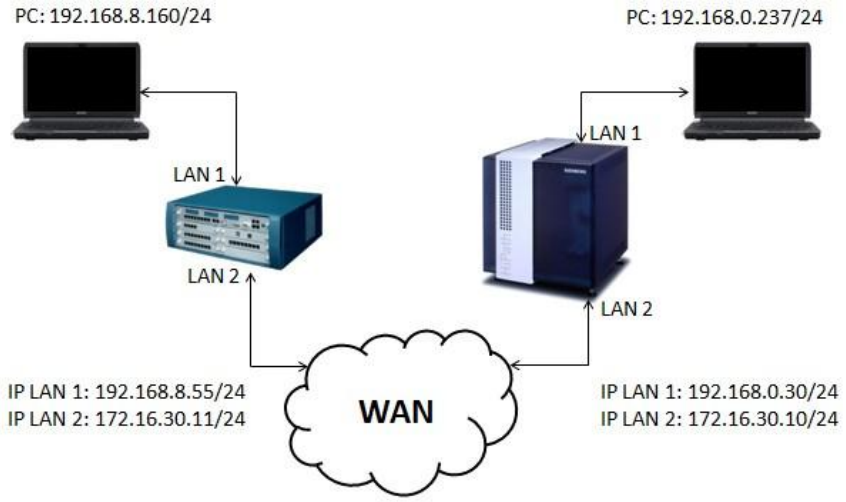
Para que o terminal esteja preparado, é necessário entrar no seu modo de administração via navegador. O aparelho utilizado foi o OpenStage 60, com o protocolo de conexão HFA. Em Páginas do Administrador, *System*, *Security*, Signaling transport main, atribuir a opção TLS.



32 – Habilitação do terminal OpenStage para segurança

4.3 VPN

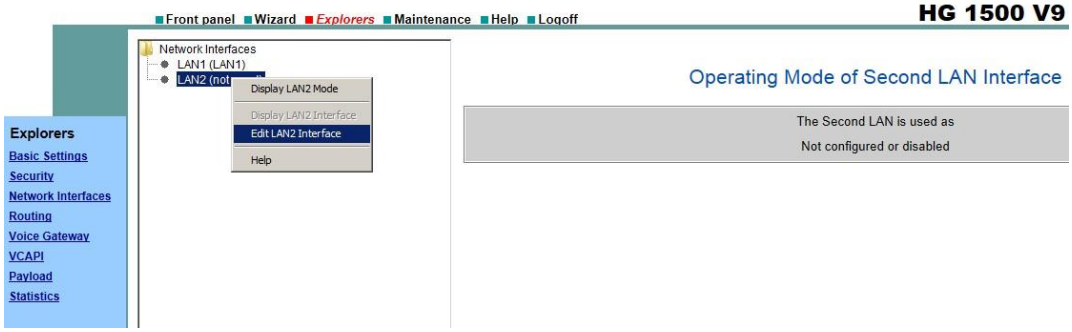
Para demonstrar uma configuração de VPN no PABX, se faz necessário ter como modelo o seguinte cenário:



33 – Cenário prático

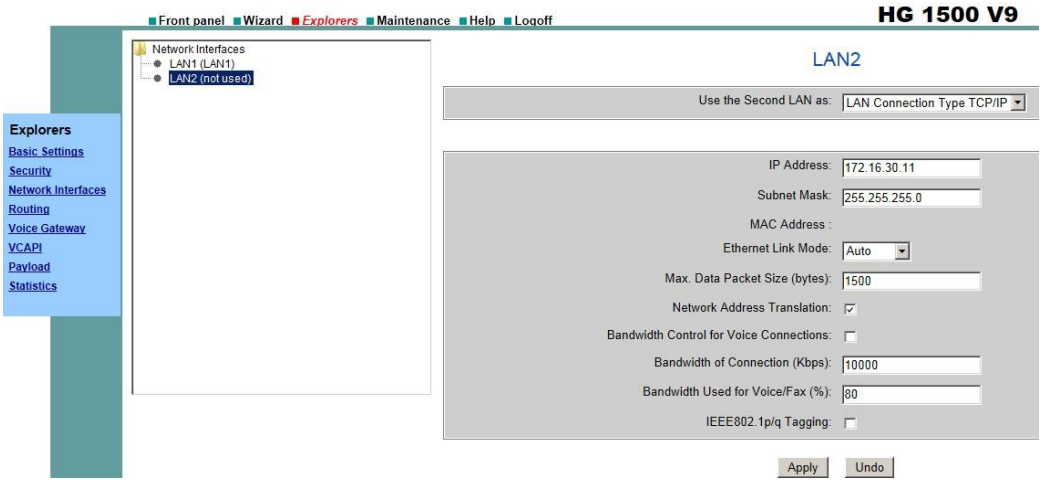
A configuração abaixo será para a central Siemens HiPath 3000 que se encontra à esquerda. Caso seja desejado concluir a prática, aplicar a configuração espelho para a central da direita.

Para ativar tal VPN, é necessário ativar a segunda porta LAN do módulo HG. Esta servirá como interface com a rede externa (WAN). Para configurá-la, entrar em *Network Interfaces*, clicar com o botão direito do mouse sobre LAN2 e selecionar a opção *Edit LAN2 Interface*.



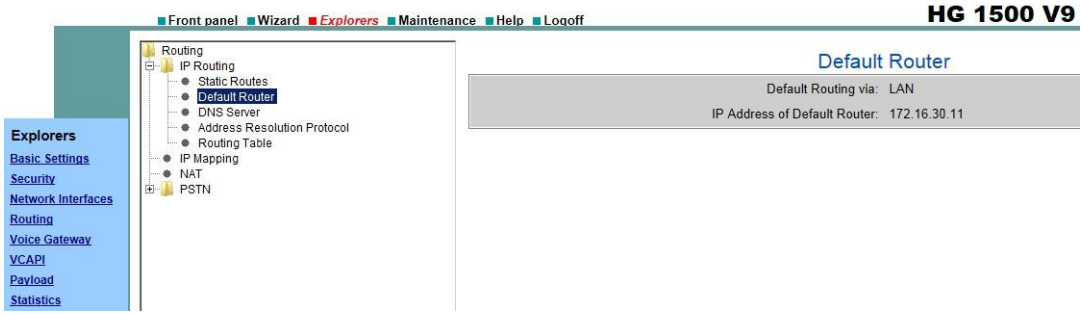
34 – Ativando a LAN2, que servirá para funções de WAN

No campo *Use the Second LAN as*, configurar com o parâmetro *LAN Connection Type TCP/IP*. Em *IP Address*, atribuir o endereço da interface e, em *Subnet Mask*, o respectivo MAC Address. A opção *Network Address Translation*, que é a permissão ao NAT, deve estar marcada.



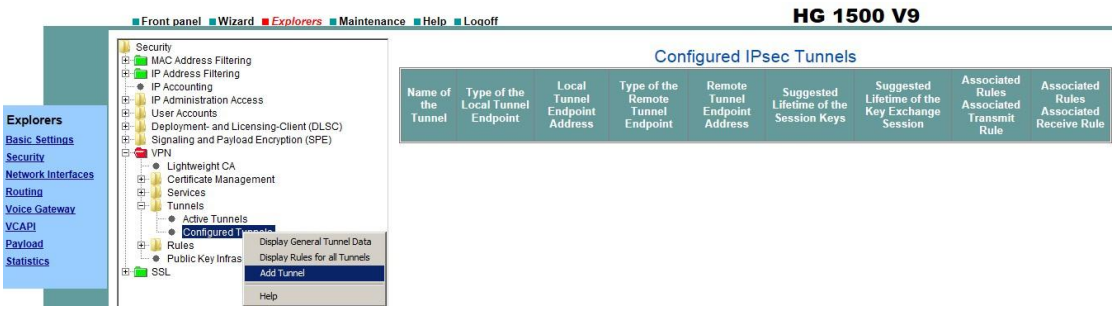
35 – Configurando a LAN2

Note que, ao configurar a LAN2, o endereço de gateway da rede, em *Routing*, *Default Router*, passa a ser o configurado na LAN2.



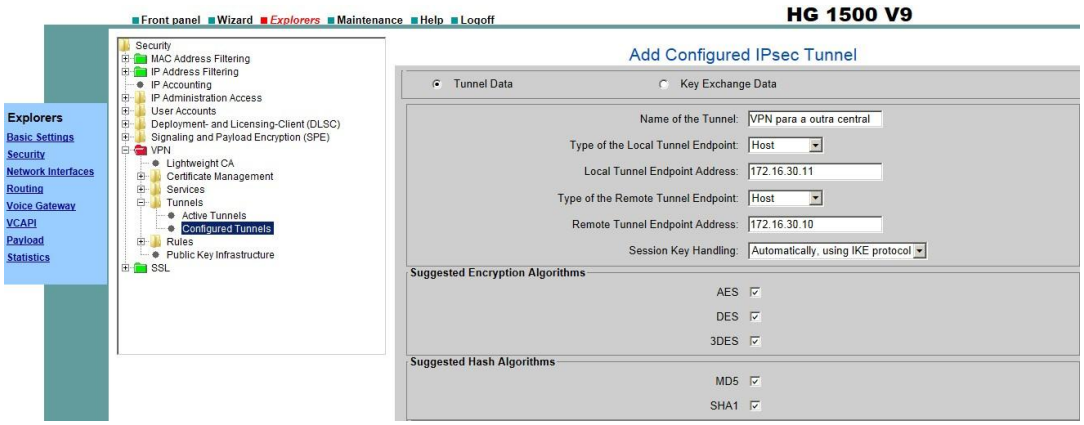
36 – Configurando o gateway da LAN

Para a configuração do tunelamento, acessar *Security*, *VPN*, *Tunnels*, clicar com o botão direito do mouse sobre *Configured Tunnels* e selecionar a opção *Add Tunnel.*



37 – Adicionando o túnel VPN

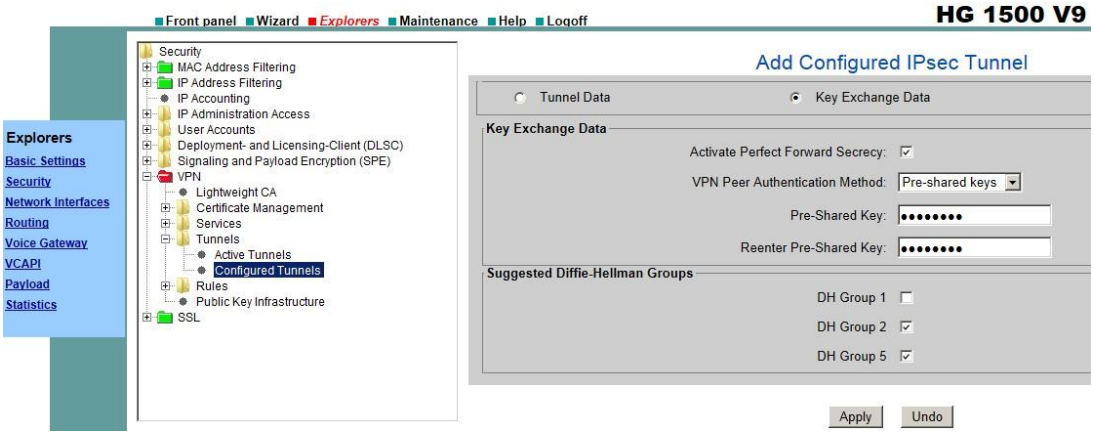
Na configuração do túnel, primeiramente, marcar a opção *Tunnel Data*. Em *Name of the Tunnel*, atribuir um nome sugestivo ao túnel VPN criado. Nas opções *Type of the Local Tunnel Endpoint*, e *Type of the Remote Tunnel Endpoint*, selecionar *Host*. Em *Local Tunnel Endpoint Address*, inserir o endereço da LAN2 da própria central. Já em *Remote Tunnel Endpoint Address*, deve ser posto o endereço da LAN2 da HG remota. Todos os demais parâmetros devem estar marcados conforme a figura abaixo.



38 – Configurando o túnel VPN

O tunelamento criado deve ter a mesma senha de chave de criptografia em ambos os módulos HG. Logo após a configuração do passo anterior, a configuração automaticamente é direcionada para tal ação.

A opção *Key Exchange Data* deve estar marcada, assim como os campos *Activate Perfect Forward Secrecy*, *DH Group 2* e *DH Group 5*. Em *VPN Peer Authentication Method*, selecionar a opção *Pre-shared Keys*. Nos campos *Pre-Shared Key* e *Reenter Pre-shared Key*, atribuir a senha de chave de criptografia. Vale lembrar que estes dois campos devem estar igualmente configurados no outro módulo HG.

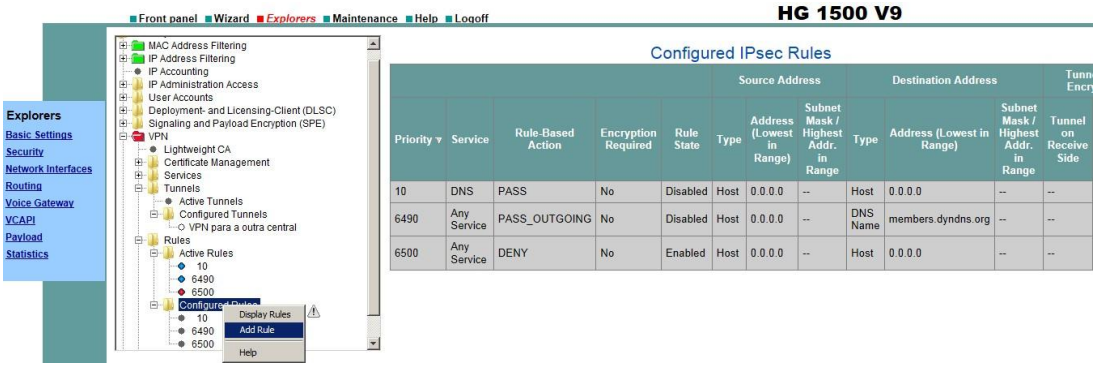


39 – Atribuindo as senhas das chaves de criptografia

Agora, serão criadas 3 regras para o túnel VPN. São elas:

- Reconhecimento da rede LAN;
- Reconhecimento de tráfego para a rede LAN remota;
- Reconhecimento de tráfego da rede LAN remota;

Para criar uma regra, é necessário ir a *Security*, *VPN*, *Rules*, clicar com o botão direito do mouse sobre *Configured Rules*, e selecionar a opção *Add Rule*.

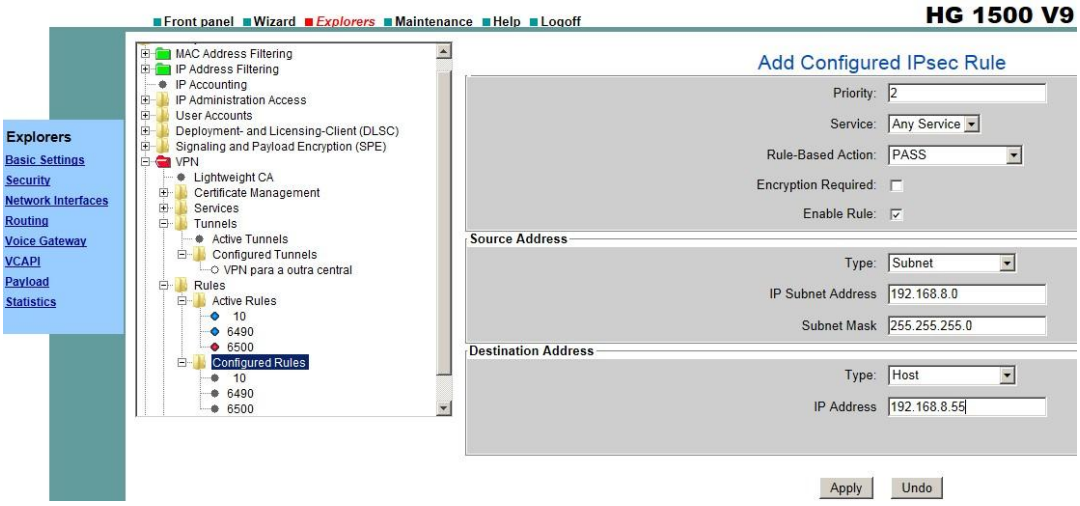


40 – Adicionando as regras IPSec

A primeira regra, que é pertinente ao reconhecimento da rede LAN, deve ser configurada da seguinte forma:

- Campo *Priority*: 2;
- *Service*: *Any Service*;
- *Rule-Based Action*: *PASS*;
- *Encryption Required*: desmarcada;
- *Enable Rule*: marcada;

- *Type*: *Subnet;*
- *IP Subnet Address*: IP de rede da LAN local;
- *Subnet Mask*: máscara de sub-rede da LAN local;
- *Type*: *Host*;
- *IP Address*: IP da LAN1 do HG local;

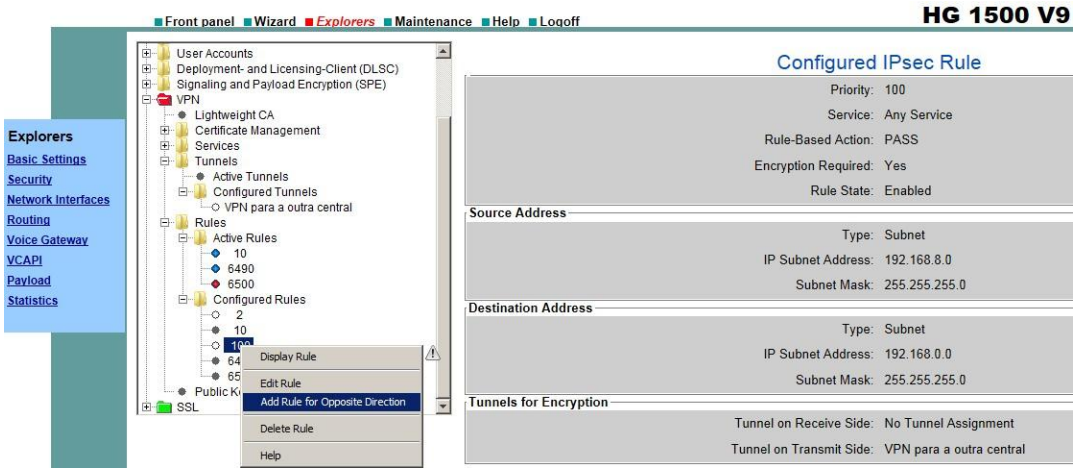


41 – Configurando a primeira regra IPSec

Para a segunda regra, referente reconhecimento de tráfego para a rede LAN remota, configurar conforme as recomendações abaixo:

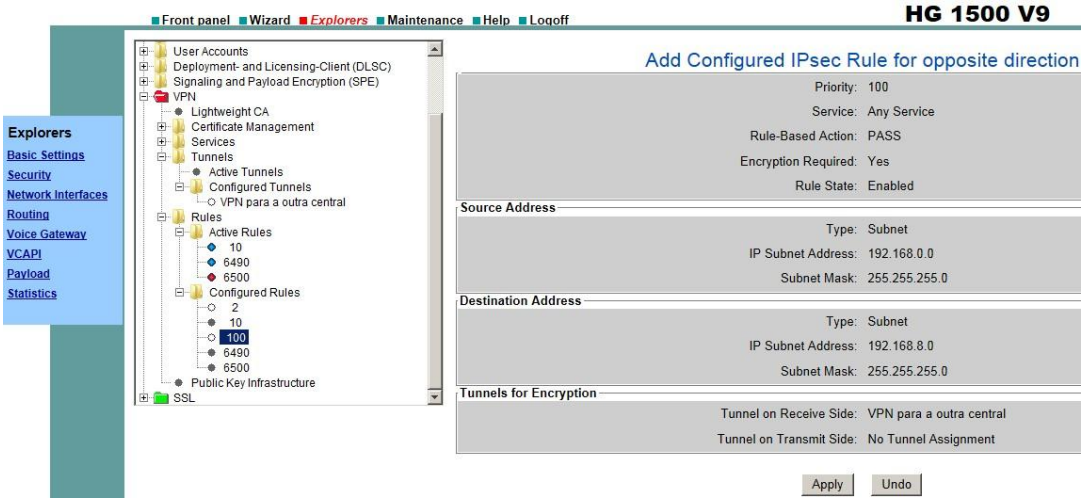
- Campo *Priority*: 100;
- *Service*: *Any Service*;
- *Rule-Based Action*: *PASS*;
- *Encryption Required*: marcada;
- *Enable Rule*: marcada;
- *Type*: *Subnet;*
- *IP Subnet Address*: IP de rede da LAN local;
- *Subnet Mask*: máscara de sub-rede da LAN local;
- *Type*: *Subnet*;
- *IP Subnet Address*: IP de rede da LAN remota;
- *Subnet Mask*: máscara de sub-rede da LAN remota;
- *Tunnel on Receive Side: No Tunnel Assignment;*
- *Tunnel on Transmit Side:* Nome do túnel criado;

Ainda conforme a figura abaixo, a regra oposta deve ser criada, para que seja criado o reconhecimento de tráfego para a rede LAN remota. Para tal, clicar com o botão direito do mouse sobre a regra, e selecionar a opção *Add Rule for Opposite Direction.*



42 – Adicionando a regra oposta

Abaixo, a regra oposta:

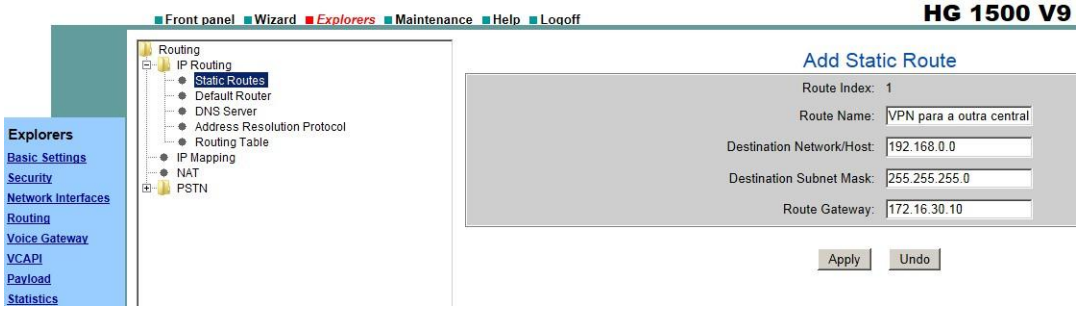


43 – Visualizando a regra oposta

Em seguida, deve ser adicionada uma rota estática para a rede remota, utilizando o endereço da LAN2 da HG remota. Ir a *Routing*, *IP Routing*, clicar com o botão direito sobre *Add Static Route.*

44 – Adicionando rota estática para rede remota

Em *Route Name*, configurar um nome conveniente. No campo *Destination Network/Host*, inserir o endereço de rede da LAN remota. Em *Destination Subnet Mask*, discriminar a máscara de sub-rede da LAN remota. Por fim, em *Route Gateway*, configurar o endereço da LAN2 da HG remota, que servirá como porta de entrada à LAN remota.

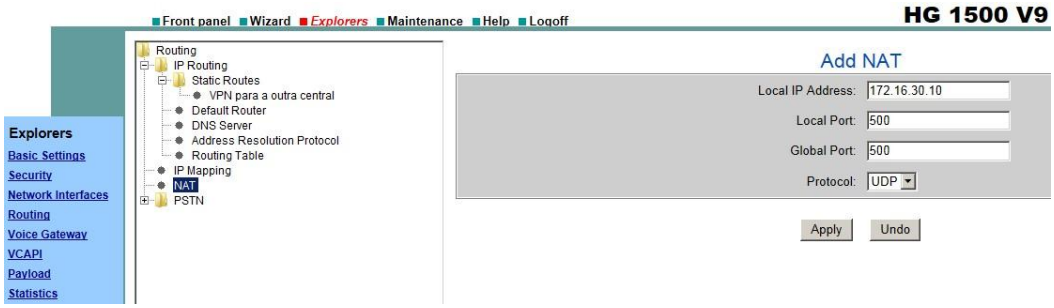


45 – Configurando a rota estática

Com o objetivo de permitir o redirecionamento do tráfego externo da rede remota para a rede interna, e vice-versa, deve ser criada uma regra de NAT. Para tal, ir a *Routing*, *IP Routing*, clicar com o botão direito do mouse sobre a opção NAT, e selecionar *Add NAT*.

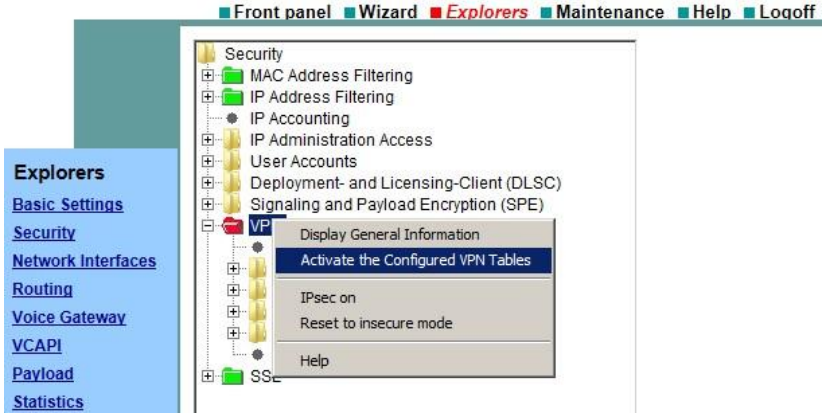
46 – Adicionando a regra de NAT

Em *Local IP Address*, atribuir o endereço da LAN2 do HG remoto. Nos campos *Local Port e Global Port*, atribuir o valor 500. Em *Protocol*, selecionar o protocolo *UDP*.



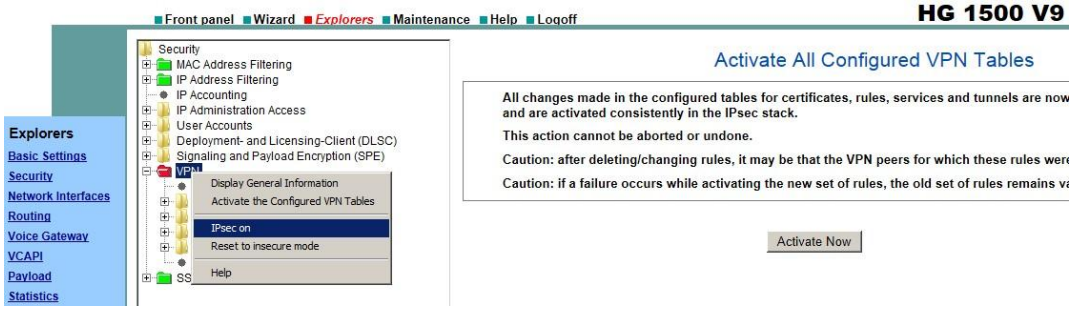
47 – Configurando o NAT

Os passos finais são para a ativação da VPN. Primeiramente, em *Security*, clicar com o botão direito do mouse sobre *VPN* e selecionar a opção *Activate the Configured VPN Tables*.



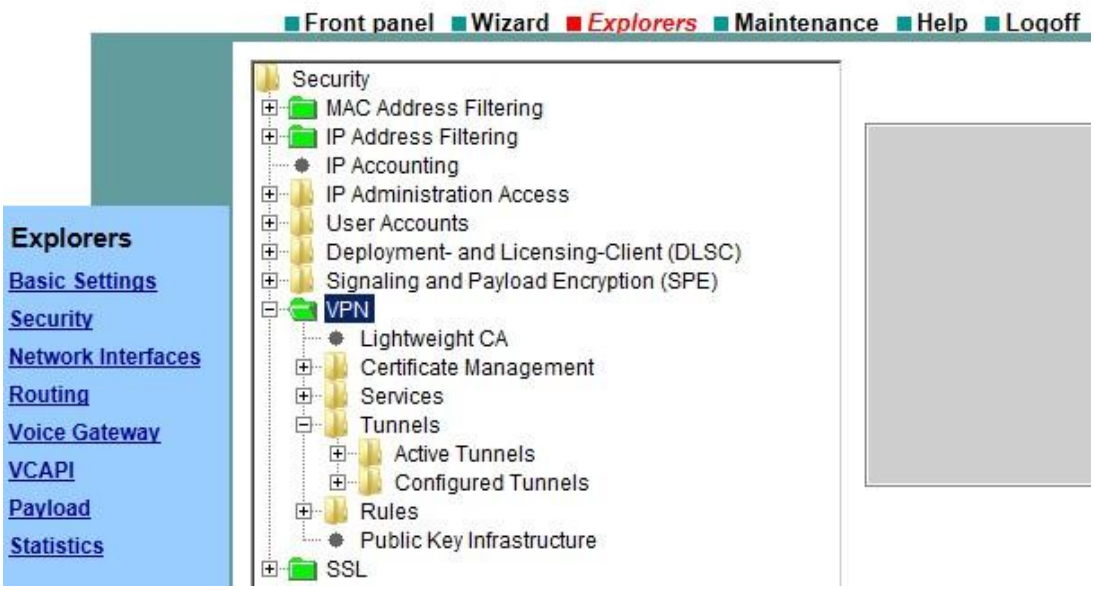
48 – Ativando as regras de VPN

Na sequência, ativar o protocolo IPsec. Para tal, também clicar com o botão direito do mouse sobre *VPN* e selecionar a opção *IPsec on*. Em seguida, clicar em *Activate Now*.



49 – Colocando a VPN em funcionamento

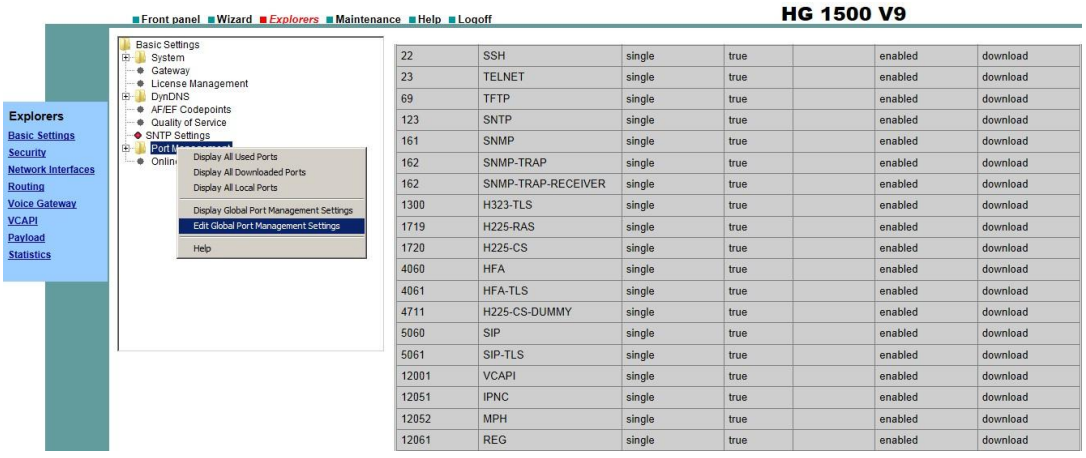
O resultado é a VPN ativa, com a pasta verde.



50 – Verificando o estado da VPN

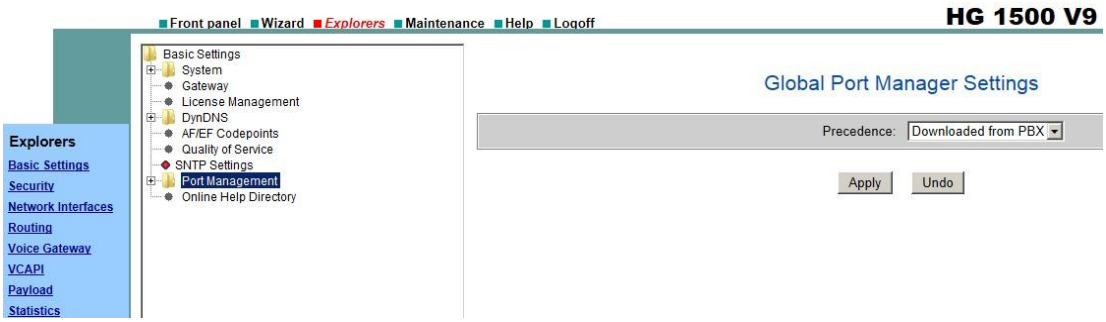
4.4 GERENCIAMENTO DE PORTAS

O módulo HG traz uma relação de todas as portas que são permitidas, tanto para o TCP, quanto para o UDP. Para visualizar, acessar *Basic Settings* e clicar sobre Port Management. Também é possível fazer alteração na tabela, enviando alguns padrões que são pré-configurados no PABX (porém, não é recomendado). Para este último procedimento, clicar com o botão direito do mouse sobre Port Management e selecionar *Edit Global Port Management Settings*. Na sequência, no campo *Precedence*, indicar o parâmetro *Downloaded from PBX*.



22	SSH	single	true		enabled	download
23	TELNET	single	true		enabled	download
69	TFTP	single	true		enabled	download
123	SNTP	single	true		enabled	download
161	SNMP	single	true		enabled	download
162	SNMP-TRAP	single	true		enabled	download
162	SNMP-TRAP-RECEIVER	single	true		enabled	download
1300	H323-TLS	single	true		enabled	download
1719	H225-RAS	single	true		enabled	download
1720	H225-CS	single	true		enabled	download
4060	HFA	single	true		enabled	download
4061	HFA-TLS	single	true		enabled	download
4711	H225-CS-DUMMY	single	true		enabled	download
5060	SIP	single	true		enabled	download
5061	SIP-TLS	single	true		enabled	download
12001	VCAPI	single	true		enabled	download
12051	IPNC	single	true		enabled	download
12052	MPH	single	true		enabled	download
12061	REG	single	true		enabled	download

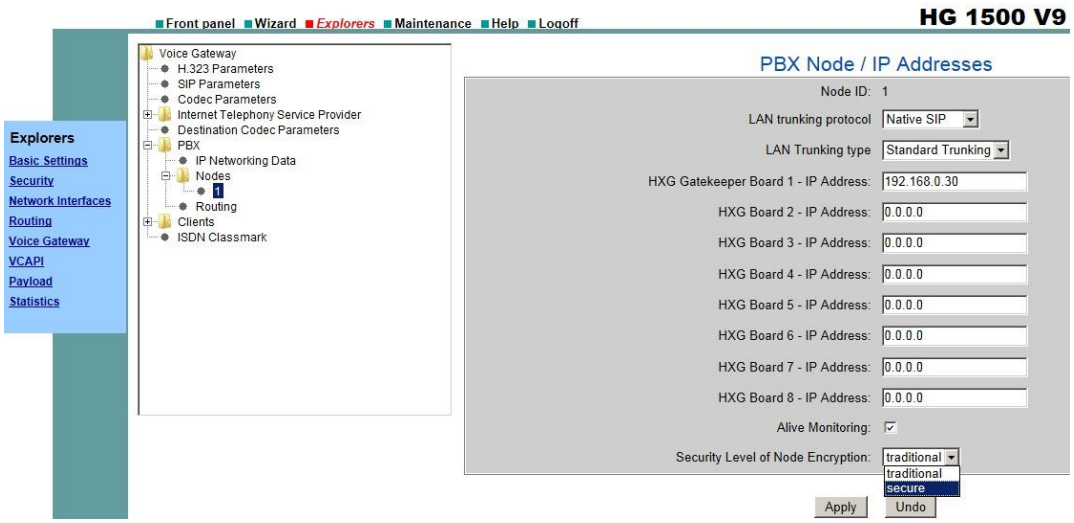
51 – Edição das portas liberadas no módulo VoIP do PABX



52 – Importando as regras de liberação de portas do PABX

4.5 SEGURANÇA NA INTERLIGAÇÃO SIMPLES

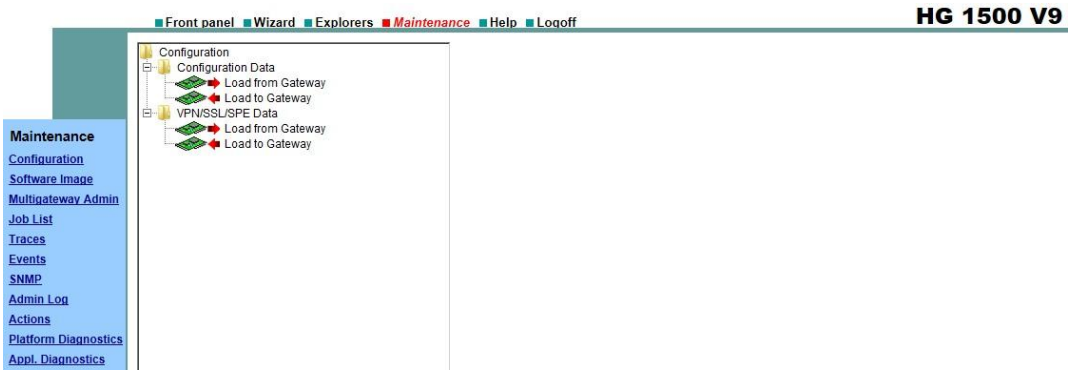
O conceito de interligação de centrais Siemens HiPath 3000 é que, para cada central a ser conectada, é necessária a criação de um nó. Este nó pode ser criptografado, caso o SPE esteja ativo nas centrais interligadas. Para o reconhecimento do SPE no nó, é necessário entrar em *Voice Gateway*, *PBX*, *Nodes*, clicar com o botão direito do mouse sobre o nó, requisitar a edição do nó. Após entrar na tela de edição do nó, em *Security Level of Node Encryption*, selecionar a opção *secure*.



53 – Parâmetro de segurança na interligação simples

4.6 BACKUP E RESTAURAÇÃO DAS CONFIGURAÇÕES

O módulo HG possui uma área dedicada à manutenção, que é a guia *Maintenance*. Em *Configuration*, é possível realizar o backup e a restauração, tanto das configurações completas do módulo HG, quanto apenas da VPN, parâmetros de SSL e SPE criados.



54 – Backup e restauração das configurações

4.7 TRÁFEGO ADICIONAL DEVIDO A SEGURANÇA

Abaixo, segue um estudo da diferença na largura de banda necessária para o tráfego da voz, por canal de comunicação, sem segurança (RTP) e com segurança (SRTP). Quanto maior a compressão dada pelo codec, maior é o percentual de consumo adicional.

Exigência maior de largura de banda através do SRTP

A tabela mostra uma vista geral necessidade maior de largura de banda através do SRTP. Supõe-se um aumento de 70 bytes na quantidade de dados devido a RTP, UDP, IP, 802.1Q VLAN Tagging e MAC (incl. preâmbulo, FCS). Além disso, há um aumento de 10 bytes devido ao SRTP. Assim, o aumento total é de 80 bytes.

Codec de voz	Duração de Sample	Payload	Tamanho do pacote de dados de Ethernet	RTP Largura de banda de Ethernet, incl. preâmbulo	Largura de banda de Ethernet SRTP, incl. Preâmbulo	SRTP Maior largura de banda de Ethernet
	(ms)	(bytes)	(bytes)	(kBit/s)	(kBit/s)	(%)
G.711	20	160	240	92	96	4,3
	40	320	400	78	80	2,6
	60	480	560	73,3	74,7	1,9
G.723.1	30	24	104	25,1	27,7	10,4
G.723.1A	60	48	128	15,7	17,1	8,9
G.729A	20	20	100	36	40	11,1
	40	40	120	22	24	9,1
	60	60	140	17,3	18,7	8,1
G.729A DMC Master Call	100	6	86	6,1	6,9	13,1
G.711 DMC Master Call	100	11	91	6,5	7,3	12,3
G.723 DMC Master Call	90	6	86	6,8	7,6	11,8

55 – Consumo de banda com parâmetros de segurança

5 CONCLUSÃO

Foi apresentado um estudo geral sobre os tipos de ameaças, mecanismos de prevenção e caso prático de implementação, sobre a segurança nas comunicações VoIP. O crescente número de ataques às redes deste tipo justifica tal estudo. A consideração do reforço da segurança em redes já existentes, e o planejamento adequado de novas redes para o suporte dos mecanismos de segurança, são fundamentais.

Este estudo mostra que a programação dos parâmetros de segurança, tendo em vista o benefício que traz, não é tão trabalhosa quanto parece. Nem todos os mecanismos e programações para evitar possíveis ataques precisam ser considerados simultaneamente; entretanto, quanto maior a quantidade de parâmetros de segurança que são programados, menores são as chances de um intruso invadir as suas comunicações VoIP.

6 REFERÊNCIAS BIBLIOGRÁFICAS

DWIVEDI, Himanshu. **Hacking VoIP:** protocols, attacks, and countermeasures. San Francisco, CA: No Starch Press, 2009.

NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

ODOM, Wendell. **CCENT/CCNA ICND 1.** Rio de Janeiro: Alta Books editora, 2008.

ODOM, Wendell. **CCENT/CCNA ICND 2.** Rio de Janeiro: Alta Books editora, 2008.

PORTER, Thomas et al. **Practical VoIP Security**. Rockland, MA: Syngress Publishing Inc, 2006

ROSENBERG, J. et al. **RFC 3261:** SIP: Session Initiation Protocol. IETF, 2002